Algebraische Zahlentheorie

Matthias Künzer

Universität Stuttgart

13. Februar 2025

Inhalt

Verzeichnis der Sätze und einiger Lemmata

Vorwort

Der Ring Z

Im Körper der rationalen Zahlen $\mathbf{Q}$ liegt der Teilring der ganzen Zahlen $\mathbf{Z}$.

In $\mathbf{Z}$ gibt es die beiden invertierbaren Elemente -1 und $+1$. Die Gruppe $\mathrm{U}(\mathbf{Z})$ der Einheiten in $\mathbf{Z}$ ist also isomorph zur zyklischen Gruppe C_2 .

Ferner gilt in $\mathbf{Z}$ das Gesetz der eindeutigen Primfaktorzerlegung.

Der Ring $\mathbf{Z}[\zeta_5]$

Sei nun $\zeta_5 := \exp(2\pi\mathrm{i}/5)$. Es ist $\mathbf{Q}(\zeta_5)|\mathbf{Q}$ eine Galoiserweiterung von Grad 4.

Eine endliche Körpererweiterung von $\mathbf{Q}$ nennt man auch einen Zahlkörper. Es ist also $\mathbf{Q}(\zeta_5)$ ein Beispiel für einen Zahlkörper.

Darin liegt der Teilring $\mathbf{Z}[\zeta_5] \subseteq \mathbf{Q}(\zeta_5)$ seiner ganzen Zahlen.

Den Teilring der ganzen Zahlen in einem Zahlkörper nennt man auch einen Zahlring. Es ist also $\mathbf{Z}[\zeta_5]$ ein Beispiel für einen Zahlring.

Wir werden feststellen, daß dessen Einheitengruppe $\mathrm{U}(\mathbf{Z}[\zeta_5])$ isomorph ist zu $\mathbf{Z} \times \mathrm{C}_{10}$, wobei der verwendete Isomorphismus $-\zeta_5$ auf einen Erzeuger des direkten Faktors C_{10} schickt.

Allgemein werden wir die Struktur der Einheitengruppe in einem gegebenen Zahlring recht genau bestimmen; sie ist endlich erzeugt, und man kennt den Rang des freien Anteils.

In $\mathbf{Z}[\zeta_5]$ gilt ferner die eindeutige Primfaktorzerlegung.

Der Ring $\mathbf{Z}[\zeta_p]$

Die eindeutige Primfaktorzerlegung gilt aber im allgemeinen nicht mehr in $\mathbf{Z}[\zeta_p]$ für p prim. Genauer gesagt, sie gilt für $p \leqslant 19$, sie gilt nicht für $p \geqslant 23$; cf. **[10]**.

Das liegt letzterenfalls an der Existenz von Primidealen in $\mathbf{Z}[\zeta_p]$, die keine Hauptideale sind. Man kann aus den Primidealen eine Gruppe bilden und aus dieser die von den Hauptidealen gelieferte Untergruppe herausfaktorisieren; man erhält so die Klassengruppe. Wenn diese Klassengruppe Ordnung 1 hat, dann liegt ein Hauptidealbereich vor, und folglich gilt darin die eindeutige Primfaktorzerlegung.

Für jeden Zahlring hat die Klassengruppe immerhin noch endliche Ordnung.

Diese endliche Ordnung der Klassengruppe von $\mathbf{Z}[\zeta_p]$ ist aber im allgemeinen unbekannt, eine diesbezügliche Teilbarkeitsaussage ist Gegenstand der Kummer-Vandiver-Vermutung. Ohne Begründung sei angeführt, daß die Klassengruppe von $\mathbf{Z}$ Ordnung 1 hat, von $\mathbf{Z}[\zeta_5]$ Ordnung 1, von $\mathbf{Z}[\zeta_{23}]$ Ordnung 3, von $\mathbf{Z}[\zeta_{67}]$ Ordnung 853513, etc.

Dagegen gilt in $\mathbf{Z}[\zeta_p]$, wie auch allgemein in jedem Zahlring, die eindeutige Primideal faktorzerlegung.

Organisatorisches

Dieses Skript lehnt sich an das erste Kapitel des Buches von Neukirch [**11**] an. Die Verantwortung für Fehler und Unklarheiten im vorliegenden Skript trage ich natürlich selbst.

Vorausgesetzt werden Kenntnisse der Algebra, insbesondere der Galoistheorie; cf. e.g. [**5**]. Der Elementarteilersatz wird eine Rolle spielen ; cf. e.g. [**4,** §1]. Den Begriff eines Moduls über einem Ring findet man e.g. in [**7,** §1.2]. In §3 werden Kenntnisse über $\mathbf{R}^n$ aus der Analysis herangezogen.

Auf Übungen und Lösungen wird im Skript manchmal Bezug genommen, sie sind daher als Bestandteil des Skripts anzusehen.

Dank geht an Wolfgang Kimmerle für seine Vorlesung zur Algebraischen Zahlentheorie, die mein Interesse weckte. Dank geht an Simon Klenk für Diskussionen über das erste Kapitel von Neukirchs Buch [**11**]. Dank geht an Fabian Hartkopf für zahlreiche Korrekturen und Verbesserungen. Dank geht an Vanda Eggert, Nora Krauss, Clemens Mayer, Sebastian Nitsche, Mathias Ritter, Elias Schwesig, Monika Truong und Cornelia Vogel für Korrekturen und Verbesserungen.

Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, im Wintersemester 2014/15 (und später)

Matthias Künzer

Konventionen. Seien X und Y Mengen. Sei R ein kommutativer Ring.

- Es stehe "für $x \in X$" kurz für "für alle $x \in X$".
- Es bedeute $Y \subset X$, daß $Y \subseteq X$ und $Y \neq X$.
- Ist X endlich, so bezeichne $|X|$ die Anzahl ihrer Elemente.
- Sei $(X, \leqslant)$ ein Poset, i.e. eine teilgeordnete Menge. Es heißt $x \in X$ *minimal*, falls es kein $y \in X$ mit $y < x$ gibt. Es heißt $x \in X$ *initial*, falls $x \leqslant z$ für alle $z \in X$ gilt. Es heißt $x \in X$ *maximal*, falls es kein $y \in X$ mit $x < y$ gibt. Es heißt $x \in X$ *terminal*, falls $z \leqslant x$ für alle $z \in X$ gilt. Es existieren höchstens ein initiales und höchstens ein terminales Element in X. Für $a \in X$ schreiben wir $X_{>a} := \{\, x \in X : x > a \,\}$, etc.
- Wir schreiben Abbildungen links. I.e. ist $X \xrightarrow{f} Y$ eine Abbildung und $x \in X$, so bezeichnet $f(x)$ oder fx das Bild von x unter f.
- Sei $f : X \longrightarrow Y$ eine Abbildung. Sei $X' \subseteq X$, $Y' \subseteq Y$ und $f(X') \subseteq Y'$. Wir schreiben $f|_{X'}^{Y'} : X' \longrightarrow Y'$, $x' \longmapsto f(x')$ für die Einschränkung. Ist $Y' = Y$, so schreiben wir auch $f|_{X'} := f|_{X'}^{Y}$. Ist $X' = X$, so schreiben wir auch $f|^{Y'} := f|_{X}^{Y'}$.
- Die identische Abbildung auf X wird id_X, 1_X, oder, falls keine Verwechslungsgefahr besteht, id oder 1 geschrieben.
- Ist $X \subseteq Y$, so schreiben wir die Inklusionsabbildung $\mathrm{id}_Y|_X : X \longrightarrow Y$, $x \longmapsto x$ auch symbolisch als $X \hookrightarrow Y$.
- Sind x, y Elemente einer Menge, so sei $\partial_{x,y} := 1$ falls $x = y$ und $\partial_{x,y} := 0$ falls $x \neq y$.
- Sind $(\, x_i : i \in I)$ und $(\, y_j : j \in J)$ Tupel von Elementen einer Menge, für indizierende Mengen I und J, dann sei $(\, x_i : i \in I) \sqcup (\, y_j : j \in J)$ das konkatenierte Tupel, welches, wenn als Funktion auf $I \sqcup J$ aufgefaßt, ein Element $i \in I$ auf x_i und ein Element $j \in J$ auf y_j schickt.
- Sind a, $b \in \mathbf{Z}$, so schreiben wir $[a, b] := \{z \in \mathbf{Z} : a \leqslant z \leqslant b\}$ für das ganzzahlige Intervall.
- Es bezeichnet $\varphi(n) := |\mathrm{U}(\mathbf{Z}/(n))|$ den Wert der Eulerschen phi-Funktion bei $n \in \mathbf{Z}_{\geqslant 1}$, i.e. die Anzahl der zu n teilerfremden Zahlen in $[1, n]$.
- In $\mathbf{Z} \sqcup \{\infty\}$ gelte $k \leqslant \infty$ und $k + \infty = \infty$ für alle $k \in \mathbf{Z} \sqcup \{\infty\}$.
- Wird ein Element $z \in \mathbf{Z}$ als Element von R angesehen, so ist damit das Bild dieses Elements unter dem eindeutigen Ringmorphismus $\mathbf{Z} \longrightarrow R$ zu verstehen.
- Schreibe $R^\times := R \smallsetminus \{0\}$. Allgemeiner, ist $\mathfrak{a} \subseteq R$ ein Ideal, so schreibe $\mathfrak{a}^\times := \mathfrak{a} \smallsetminus \{0\}$.
- Es bezeichnet $\mathrm{U}(R) = \{\, a \in R : (a) = R \,\}$ die Einheitengruppe von R.
- Ist S ein kommutativer Ring und $R \subseteq S$ darin ein Teilring, so sprechen wir von einer Ringerweiterung $S|R$.
- Sind L und K Körper und ist dabei $K \subseteq L$ ein Teilkörper, so sprechen wir von einer Körpererweiterung $L|K$. Diese heißt endlich, falls L ein endlichdimensionaler K-Vektorraum ist.

  Vorsicht, eine endliche Körpererweiterung ist nicht notwendig eine Erweiterung endlicher Körper.
- Für $n \geqslant 1$ und $a_1, \ldots, a_n \in R$ schreiben wir $(a_1, \ldots, a_n) := \{\, r_1 a_1 + \cdots + r_n a_n : r_i \in R \text{ für } i \in [1, n] \,\} \subseteq R$ für das von diesen Elementen erzeugte Ideal. Ein Ideal von dieser Form heißt endlich erzeugt. E.g. ist jedes Hauptideal in R von der Form (a) für ein geeignetes $a \in R$. Alternativ schreiben wir auch $Ra = (a)$.
- Sind a, b, $r \in R$, so bedeute $a \equiv_r b$, daß $a - b \in (r)$ ist.

  Ist I ein Ideal in R und sind a, $b \in R$, so bedeute $a \equiv_I b$, daß $a - b \in I$ ist. Insbesondere ist $a \equiv_{(r)} b$ äquivalent zu $a \equiv_r b$.

- Es heißt R Integritätsbereich, wenn $1_R \neq 0_R$ ist und R nullteilerfrei ist, i.e. wenn für $a \in R^\times$ die Abbildung $\lambda_r : R \to R$, $r \mapsto ar$ injektiv ist. Diesenfalls bezeichne $\mathrm{Quot}(R)$ seinen Quotientenkörper.
- Es bezeichnet $\mathrm{Ideale}(R)$ die teilgeordnete Menge der Ideale von R. Es bezeichnet $\mathrm{Ideale}^\times(R) := \mathrm{Ideale}(R) \smallsetminus \{(0)\}$. Es bezeichnet $\mathrm{Ideale}_{\mathrm{prim}}(R) \subseteq \mathrm{Ideale}(R)$ die Teilmenge der Primideale von R, i.e. der Ideale $\mathfrak{p} \subseteq R$, für welche $R/\mathfrak{p}$ ein Integritätsbereich ist. Es bezeichnet $\mathrm{Ideale}^\times_{\mathrm{prim}}(R) := \mathrm{Ideale}_{\mathrm{prim}}(R) \smallsetminus \{(0)\}$. Unter einem maximalen Ideal in R verstehen wir ein maximales Element $\mathfrak{m}$ von $\mathrm{Ideale}(R) \smallsetminus \{(1)\}$, i.e. ein Ideal $\mathfrak{m}$, für welches $R/\mathfrak{m}$ ein Körper ist. Maximale Ideale sind prim.
- Sei M ein R-Modul.

  Für $n \geqslant 0$ schreiben wir $M^{\oplus n} := \bigoplus_{i\in[1,n]} M$. Speziell ist $M^{\oplus 0} = \{0\} =: 0$ der Nullmodul.

  Für eine Menge I schreiben wir

  $$M^{\oplus I} := \bigoplus_{i\in I} M = \{\, (m_i)_{i\in I} \,:\, m_i \in M \text{ für } i \in I \text{ und } \{\, i \in I \,:\, m_i \neq 0 \,\} \text{ endlich} \,\}$$

  für den R-Modul, der aus den I-indizierten Tupeln $(m_i)_{i\in I}$ mit Einträgen in M mit endlichem Träger $\{\, i \in I \,:\, m_i \neq 0 \,\}$ besteht. Wir schreiben auch kurz $(m_i)_i := (m_i)_{i\in I}$. Die Operationen sind eintragsweise definiert, i.e. $r(m_i)_i + r'(m'_i)_i = (rm_i + r'm'_i)_i$ für $r, r' \in R$ und $(m_i)_i, (m'_i)_i \in M^{\oplus I}$.

  Ist $R = K$ ein Körper, so schreiben wir alternativ auch $K^n = K^{\oplus n}$.
- Ist M ein R-Modul mit $M \simeq R^{\oplus k}$ für ein $k \geqslant 0$, so heißt M *endlich erzeugt frei* und $\mathrm{rk}_R M := k$ der *Rang* von M. Cf. Aufgabe 13.(1).
- Die Injektivität einer linearen Abbildung wird zuweilen mit $\hookrightarrow$, die Surjektivität mit $\twoheadrightarrow$ angedeutet.
- Gegeben seinen R-Moduln M', M, M'' und R-lineare Abbildungen $M' \xrightarrow{u} M \xrightarrow{v} M''$. Diese Sequenz der zwei aufeinanderfolgenden R-linearen Abbildungen heißt exakt bei M, wenn $u(M') = \mathrm{Kern}(v)$ ist.

  Allgemein heißt eine Sequenz von R-Moduln und R-linearen Abbildungen exakt, wenn sie an jeder Stelle exakt ist.
- Ein Element $a \in R$ heißt prim, falls $R/(a)$ ein Integritätsbereich ist, i.e. falls $(a) \subseteq R$ ein Primideal ist.
- Ein Element $a \in R$ heißt irreduzibel, falls $a \notin \mathrm{U}(R)$ liegt, aber aus $a = bc$ mit $b, c \in R$ bereits $b \in \mathrm{U}(R)$ oder $c \in \mathrm{U}(R)$ folgt.
- Ist $p \in R$ prim und $x \in R$, so schreiben wir $\mathrm{v}_p(x) := \max\{\, \alpha \in \mathbf{Z}_{\geqslant 0} \,:\, x \in (p^\alpha) \,\}$ für die Bewertung (engl. valuation) von x bei p, sofern existent.
- Ist $n \in \mathbf{Z}$ und $p \in \mathbf{Z}_{>0}$ prim, so schreiben wir $n[p] := p^{\mathrm{v}_p(n)}$.
- Für $f = f(X) \in R[X] \smallsetminus \{0\}$ bezeichnet $\deg(f)$ den Grad von f.
- Sind $X, Y, Z \subseteq R$, so schreiben wir $X \cdot Y := {}_{\mathbf{Z}}\langle\, x \cdot y \,:\, x \in X,\, y \in Y \,\rangle$. Ist X ein Ideal in R, so ist $X \cdot Y$ ein Ideal in R. Es ist $X \cdot Y = Y \cdot X$. Es ist $(X \cdot Y) \cdot Z = {}_{\mathbf{Z}}\langle\, x \cdot y \cdot z \,:\, x \in X,\, y \in Y,\, z \in Z \,\rangle = X \cdot (Y \cdot Z)$. Daher können wir bei mehrfachen Produkten die Klammern wegfallen lassen.
- Seien $m, n \geqslant 0$. Für $i \in [1, m]$ und $j \in [1, n]$ bezeichne $\mathrm{e}_{i,j} \in R^{m\times n}$ die Matrix, die an Position (i, j) den Eintrag 1 hat, und ansonsten 0. Sei $\mathrm{E}_n := \sum_{i\in[1,n]} \mathrm{e}_{i,i} = (\partial_{i,j})_{i,j} \in R^{n\times n}$ die Einheitsmatrix.
- Für $n \geqslant 0$ sei $\mathrm{GL}_n(R) := \{\, U \in R^{n\times n} \,:\, \text{es gibt } V \in R^{n\times n} \text{ mit } UV = \mathrm{E}_n = VU \,\}$. Vermöge Matrixmultiplikation ist dies eine Gruppe.
- Die Spur einer quadratischen Matrix B wird $\mathrm{tr}(B)$ geschrieben (engl. trace). Genauso die Spur eines Endomorphismus eines endlichdimensionalen Vektorraums.

- Die Transponierte einer Matrix B wird B^{t} geschrieben.
- Für $n \geqslant 0$ ist das Standardskalarprodukt auf $\mathbf{R}^n$ gegeben durch $\lfloor (x_i)_i \,,\, (y_i)_i \rfloor = \sum_{i \in [1,n]} x_i \, y_i$.
- Für $n \geqslant 1$ sei $\zeta_n := \exp(2\pi \mathrm{i}/n)$. Somit ist ζ_n eine primitive n-te Einheitswurzel über $\mathbf{Q}$.
  Man kann auch annehmen, ζ_n sei eine Nullstelle von $X^n - 1$ im Zerfällungskörper E von $X^n - 1 \in \mathbf{Q}[X]$, die die Gruppe der Nullstellen von $X^n - 1$ in E erzeugt, welche Ordnung n hat, da $X^n - 1$ und $(X^n - 1)'$ teilerfremd sind, und welche als endliche Untergruppe der multiplikativen Gruppe dieses Zerfällungskörpers zyklisch ist – wenn man die Verwendung von $\mathbf{C}$ vermeiden möchte.
- Die (multiplikativ notierte) triviale Gruppe, die nur aus dem Einselement besteht, wird auch 1 geschrieben.
- Ist G eine Gruppe und $U \subseteq G$, so bedeute $U \leqslant G$, daß U eine Untergruppe von G ist, und $U \trianglelefteqslant G$, daß U ein Normalteiler von G ist.
- Ist G eine Gruppe und $M \subseteq G$ eine Teilmenge, so sei $\langle\!\langle M \rangle\!\rangle$ das Untergruppenerzeugnis von M, i.e. $\langle\!\langle M \rangle\!\rangle := \{\, m_1^{\varepsilon_1} m_2^{\varepsilon_2} \cdots m_k^{\varepsilon_k} \,:\, k \geqslant 0,\, m_i \in M \text{ und } \varepsilon_i \in \{-1, +1\} \text{ für } i \in [1,k] \,\}$ ([1]).
- Für $n \geqslant 0$ sei S_n die symmetrische Gruppe, bestehend aus Bijektionen von $[1,n]$ nach $[1,n]$; sei $\mathrm{A}_n := \mathrm{Kern}(\mathrm{sgn}) = \{\, sa \in \mathrm{S}_n \,:\, \mathrm{sgn}(\sigma) = +1 \,\} \subseteq \mathrm{S}_n$ die alternierende Gruppe.
- Für $n \geqslant 1$ sei C_n die zyklische Gruppe der Ordnung n.
- Ist $z = a + b\mathrm{i} \in \mathbf{C}$, wobei $a,\, b \in \mathbf{R}$, dann ist $\bar{z} := a - b\mathrm{i} \in \mathbf{C}$ die zu z komplex konjugierte Zahl. Ist $A = (a_{i,\,j})_{i,\,j}$ eine Matrix mit Einträgen in $\mathbf{C}$, dann schreiben wir $\bar{A} = (\bar{a}_{i,\,j})_{i,\,j}$.
- Wir bezeichnen die Kreiszahl mit π.
- Der natürliche Logarithmus wird mit ln, die Eulersche Zahl mit e bezeichnet.
- Wir verwenden ansonsten die Konventionen aus [**5**].

[1] Diese ansonsten ungebräuchliche Notation wird nur wegen der Verwechslungsgefahr mit dem Teilraumerzeugnis verwendet.

Kapitel 1

Ganzheit

1.1 Der Ring der ganzen Elemente

Sei $B|A$ eine Erweiterung kommutativer Ringe, i.e. sei B ein kommutativer Ring und $A \subseteq B$ ein Teilring.

Wir erinnern daran, daß ein A-Teilmodul M von B eine Teilmenge ist, welche 0 enthält und für welche $am + a'm' \in M$ ist für $a,\, a' \in A$ und $m,\, m' \in M$. Dieser heißt endlich erzeugt, wenn es eine endliche Teilmenge $M_0 \subseteq M$ mit

$$\{\, \textstyle\sum_{i\in[1,k]} a_i m_i \,:\, k \geqslant 0,\, a_i \in A \text{ und } m_i \in M_0 \text{ für } i \in [1,k] \,\} \;=:\; {}_A\langle M_0 \rangle \;=\; M$$

gibt.

Lemma 1 *Gegeben sei $b \in B$. Die Aussagen* (1, 2, 3) *sind äquivalent.*

(1) *Es gibt ein normiertes Polynom $f(X) \in A[X]$ mit $f(b) = 0$.*

(2) *Es ist $A[b]$ ein endlich erzeugter A-Teilmodul von B.*

(3) *Es ist $A[b]$ enthalten in einem Teilring $C \subseteq B$, welcher ein endlich erzeugter A-Modul ist.*

Beweis.

Ad (1) $\Rightarrow$ (2). Sei $n \geqslant 0$ und $f(X) = \sum_{i\in[0,n]} a_i X^i$ mit $a_n = 1$ und $f(b) = 0$ gegeben. Ist $j \geqslant 0$, so ist $b^{n+j} = -\sum_{i\in[0,n-1]} a_i b^{i+j} \in {}_A\langle\, b^i \,:\, i \in [0, n+j-1] \,\rangle$ und also

$${}_A\langle\, b^i \,:\, i \in [0, n+j] \,\rangle \;\subseteq\; {}_A\langle\, b^i \,:\, i \in [0, n+j-1] \,\rangle\,.$$

Per Induktion folgt

$${}_A\langle\, b^i \,:\, i \in [0, n+j] \,\rangle \;\subseteq\; {}_A\langle\, b^i \,:\, i \in [0, n-1] \,\rangle$$

und also

$$A[b] \;=\; \bigcup_{j\geqslant 0} {}_A\langle\, b^i \,:\, i\in[0,n+j]\,\rangle \;\subseteq\; {}_A\langle\, b^i \,:\, i\in[0,n-1]\,\rangle\;.$$

Ad (2) $\Rightarrow$ (3). Wir können $C = A[b]$ verwenden.

Ad (3) $\Rightarrow$ (1). Sei $C = {}_A\langle\, c_i \,:\, i\in[1,k]\,\rangle$ für ein $k\geqslant 0$ und gewisse $c_i\in C$. Es ist $bc_i\in C$ für $i\in[1,k]$. Also gibt es $S=(s_{i,j})_{i,j}\in A^{k\times k}$ mit $bc_i=\sum_{j\in[1,k]} s_{i,j}c_j$ für $i\in[1,k]$, i.e. mit $\sum_{j\in[1,k]}(b\partial_{i,j}-s_{i,j})c_j=0$ für $i\in[1,k]$.

Wir schreiben $T=(t_{i,j})_{i,j}:=b\mathrm{E}_k-S\in B^{k\times k}$. Es ist also $\sum_{j\in[1,k]} t_{i,j}c_j=0$ für $i\in[1,k]$.

Sei $T'=(t'_{i,j})_{i,j}\in B^{k\times k}$ die Adjunkte zu T, i.e. sei

$$t'_{v,u} \;=\; (-1)^{u+v}\det((t_{i,j})_{i\in[1,k]\smallsetminus\{v\},\, j\in[1,k]\smallsetminus\{u\}})$$

für $u,\,v\;\in\;[1,k]$. Dann gilt nach Cramerscher Regel $T'T\;=\;\det(T)\mathrm{E}_k$. I.e. es ist $\sum_{i\in[1,k]} t'_{\ell,i}t_{i,j}=\det(T)\partial_{\ell,j}$ für $j,\,\ell\,\in\,[1,k]$. Für $\ell\in[1,k]$ folgt

$$\det(T)c_\ell \;=\; \textstyle\sum_{j\in[1,k]}\det(T)\partial_{\ell,j}\,c_j \;=\; \sum_{i,\,j\,\in\,[1,k]} t'_{\ell,i}\,t_{i,j}\,c_j \;=\; 0\;,$$

also, da $1\in C={}_A\langle\, c_i \,:\, i\in[1,k]\,\rangle$, auch $\det(T)=0$.

Daher ist $f(X):=\det(X\mathrm{E}_k-S)\in A[X]$ nach der Leibnizformel ein normiertes Polynom, und es ist $f(b)=\det(b\mathrm{E}_k-S)=\det(T)=0$. ▫

Definition 2 Ein Element $b\in B$ heißt *ganz* über A, falls es einer der äquivalenten Bedingungen von Lemma 1 genügt.

Wir schreiben

$$\Gamma_B(A) \;:=\; \{\, b\in B \,:\, b \text{ ist ganz über } A\,\} \;\subseteq\; B$$

für den *ganzen Abschluß* von A in B.

Ist $K|\mathbf{Q}$ eine endliche Körpererweiterung, so wird K auch *Zahlkörper* genannt, und wir schreiben häufig auch

$$\mathcal{O}_K \;:=\; \Gamma_K(\mathbf{Z}) \;=\; \{\, x\in K \,:\, x \text{ ist ganz über } \mathbf{Z}\,\} \;\subseteq\; K$$

für den zugehörigen *Zahlring*, im Vorgriff auf Lemma 5.

Algebraische Zahlentheorie ist das Studium von $\mathcal{O}_K$. Im Vorwort wurden Beispiele genannt.

Beispiel 3

(1) Jedes Element a von A ist ganz über A, da mit dem normierten Polynom $f(X)=X-a\in A[X]$ in der Tat $f(a)=0$ ist. Es ist also $A\subseteq\Gamma_B(A)\subseteq B$.

(2) Betrachte $\mathbf{Q}|\mathbf{Z}$. Es ist $\frac{1}{2} \in \mathbf{Q}$ nicht ganz über $\mathbf{Z}$. *Annahme,* doch. Sei $n \geqslant 1$ und $f(X) = \sum_{i\in[0,n]} a_i X^i \in \mathbf{Z}[X]$ mit $a_n = 1$ und $f(\frac{1}{2}) = 0$ gefunden. Dann ist $\sum_{i\in[0,n]} a_i 2^{n-i} = 0$, und also $1 = 2(-\sum_{i\in[0,n-1]} a_i 2^{n-1-i})$. Aber 1 ist in $\mathbf{Z}$ nicht durch 2 teilbar, *Widerspruch.*

Beachte auch, daß $\frac{1}{2}$ zwar schon Nullstelle des Polynoms $2X - 1 \in \mathbf{Z}[X]$ ist, dieses aber nicht normiert ist.

(3) Betrachte $\mathbf{Q}(\mathrm{i})|\mathbf{Z}$. Es ist i ganz über $\mathbf{Z}$, da mit dem normierten Polynom $f(X) = X^2 + 1 \in \mathbf{Z}[X]$ in der Tat $f(\mathrm{i}) = 0$ ist.

(4) Betrachte $\mathbf{Q}(\sqrt{5})|\mathbf{Z}$. Sei $\alpha := (1 + \sqrt{5})/2$. Es ist $\alpha^2 = (1 + 2\sqrt{5} + 5)/4 = \alpha + 1$. Also ist α eine Nullstelle des normierten Polynoms $X^2 - X - 1 \in \mathbf{Z}[X]$. Folglich ist α ganz über $\mathbf{Z}$.

(5) Ist $B|A$ eine Körpererweiterung, so ist ein Element von B genau dann ganz über A, wenn es algebraisch über A ist.

Lemma 4 *Seien $T|S|R$ Erweiterungen kommutativer Ringe derart, daß T ein endlich erzeugter S-Modul und S ein endlich erzeugter R-Modul ist.*

Dann ist T ein endlich erzeugter R-Modul.

Beweis. Sei $S = {}_R\langle\, s_i \,:\, i \in [1,k]\,\rangle$ für ein $k \geqslant 0$ und gewisse $s_i \in S$.

Sei $T = {}_S\langle\, t_j \,:\, j \in [1,\ell]\,\rangle$ für ein $\ell \geqslant 0$ und gewisse $t_j \in T$.

Wir *behaupten* $T \stackrel{!}{=} {}_R\langle\, s_i t_j \,:\, i \in [1,k],\, j \in [1,\ell]\,\rangle$.

Sei $t \in T$ gegeben. Es ist $t = \sum_{j\in[1,\ell]} \tilde{s}_j\, t_j$ mit gewissen $\tilde{s}_j \in S$. Es ist $\tilde{s}_j = \sum_{i\in[1,k]} \tilde{r}_{j,i}\, s_i$ für gewisse $\tilde{r}_{j,i} \in R$. Zusammengenommen ist also $t = \sum_{j\in[1,\ell]} \tilde{s}_j t_j = \sum_{i\in[1,k],\, j\in[1,\ell]} \tilde{r}_{j,i}\, s_i\, t_j$. Dies zeigt die *Behauptung.* ▫

Lemma 5 *Es ist $\Gamma_B(A)$ ein Teilring von B.*

Beweis. Es ist $1 \in \Gamma_B(A)$.

Seien $u,\, v \in \Gamma_B(A)$. Es genügt, $A[u,v] \stackrel{!}{\subseteq} \Gamma_B(A)$ zu zeigen. Da für $w \in A[u,v]$ auch $A[w] \subseteq A[u,v]$ ist, genügt es dank Lemma 1.(3) zu zeigen, daß $A[u,v]$ ein endlich erzeugter A-Modul ist.

Es ist u ganz über A, also $A[u]$ ein endlich erzeugter A-Modul; cf. Lemma 1.(2). Es ist v ganz über A. Somit gibt es ein normiertes $f(X) \in A[X]$ mit $f(v) = 0$; cf. Lemma 1.(1). Nun ist $f(X)$ auch ein normiertes Polynom in $A[u][X]$. Also ist v auch ganz über $A[u]$; cf. Lemma 1.(1). Also ist $A[u,v]$ endlich erzeugt über $A[u]$; cf. Lemma 1.(2). Dank Lemma 4, angewandt auf $A[u,v] \,|\, A[u] \,|\, A$, folgt nun, daß $A[u,v]$ ein endlich erzeugter A-Modul ist. ▫

Lemma 6 *Es ist* $\Gamma_B(\Gamma_B(A)) = \Gamma_B(A)$.

Beweis. Zu zeigen ist nur $\Gamma_B(\Gamma_B(A)) \overset{!}{\subseteq} \Gamma_B(A)$. Sei $u \in \Gamma_B(\Gamma_B(A))$. Wir wollen $u \overset{!}{\in} \Gamma_B(A)$ nachweisen.

Wähle ein $n \geqslant 0$ und ein $f(X) = \sum_{i\in[0,n]} v_i X^i \in \Gamma_B(A)[X]$ mit $a_n = 1$ und $f(u) = 0$. Nun ist auch $f(X) \in A[v_0\,, \ldots\,, v_{n-1}][X]$ und also u ganz über $A[v_0\,, \ldots\,, v_{n-1}]$. Es ist v_i ganz über A für $i \in [0, n-1]$. Also ist auch v_i ganz über $A[v_0\,, \ldots\,, v_{i-1}]$ für $i \in [0, n-1]$. In der Erweiterungskette

$$A[v_0\,, \ldots\,, v_{n-1}\,, u] \,|\, A[v_0\,, \ldots\,, v_{n-1}] \,|\, A[v_0\,, \ldots\,, v_{n-2}] \,|\, \ldots \,|\, A[v_0] \,|\, A$$

ist mithin jeder Ring ein endlich erzeugter Modul über dem nächstkleineren Ring. Mit Lemma 4 folgt, daß $A[v_0\,, \ldots\,, v_{n-1}\,, u]$ ein endlich erzeugter A-Modul ist. Dank Lemma 1.(3) ist also u ganz über A, i.e. $u \in \Gamma_B(A)$. ▫

Definition 7

(1) Es heißt die Ringerweiterung $B|A$ *ganz*, falls $\Gamma_B(A) = B$ ist.

(2) Ist A ein Integritätsbereich, so heißt A *ganzabgeschlossen,* falls $\Gamma_{\mathrm{Quot}(A)}(A) = A$ ist.

Bemerkung 8

(1) Hauptidealbereiche sind ganzabgeschlossen; cf. Aufgabe 6.(1). So etwa sind $\mathbf{Z}$, $\mathbf{Z}$[i] und $\mathbf{F}_7[X]$ ganzabgeschlossen; cf. Aufgabe 6.(2).

(2) Sei A ein Integritätsbereich und B ein Körper. Dann ist $A' := \Gamma_B(A)$ ganzabgeschlossen. Denn dann ist $A \subseteq A' \subseteq \mathrm{Quot}(A') \subseteq B$; cf. Aufgabe 11.(1). Also wird

$$\Gamma_{\mathrm{Quot}(A')}(A') \;=\; \mathrm{Quot}(A') \cap \Gamma_B(A') \;\overset{\text{L. 6}}{=}\; \mathrm{Quot}(A') \cap A' \;=\; A'\,.$$

1.2 Spur und Norm

Sei K perfekt; cf. [**5,** §3.3].

Wir erinnern daran, daß Körper von Charakteristik 0 perfekt sind. Wir erinnern daran, daß endliche Körper perfekt sind. Aber z.B. $\mathbf{F}_3(X) = \mathrm{Quot}(\mathbf{F}_3[X])$ ist nicht perfekt.

Sei $L|K$ eine endliche Körpererweiterung.

1.2.1 Zerfällungskörper

Definition 9 Ist $E|L$ eine Körpererweiterung, so heißt E ein *Zerfällungskörper* von $L|K$, wenn $(1, 2)$ gelten.

(1) Es ist $E|K$ galoisch.

(2) Der kleinste Teilkörper von E, der $\sigma(L)$ enthält für alle $\sigma \in \mathrm{Gal}(E|K)$, ist E.

Beispiel 10

(1) Ist $L|K$ galoisch, dann ist L ein Zerfällungskörper von $L|K$.

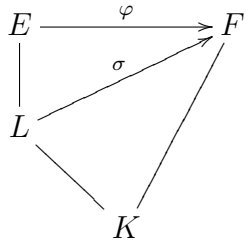
(2) Es ist $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ Zerfällungskörper von $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$; cf. Aufgabe 7.

Lemma 11

(1) *Es gibt einen Zerfällungskörper E von $L|K$ mit $E|L$ endlich.*

(2) *Sind zwei Zerfällungskörper E und E' von $L|K$ gegeben, dann gibt es einen Isomorphismus $\psi : E \longrightarrow E'$ von Körpern mit $\psi|_L^L = \mathrm{id}_L$.*

(3) *Ist E ein Zerfällungskörper von $L|K$, ist $F|K$ eine galoische endliche Körpererweiterung und ist $\sigma : L \longrightarrow F$ ein Körpermorphismus mit $\sigma|_K^K = \mathrm{id}_K$, dann gibt es einen Körpermorphismus $\varphi : E \longrightarrow F$ mit $\varphi|_L = \sigma$.*



Beweis. Da $L|K$ endlich ist, gibt es $n \geqslant 0$ und $y_1, \ldots, y_n \in L$ mit $L = K(y_1, \ldots, y_n)$. Schreibe $f(X) := \mu_{y_1, K}(X) \cdots \mu_{y_n, K}(X)$

Ad (1). Sei E ein Zerfällungskörper von $f(X) \in L[X]$; cf. [**5,** §2.5.1, §2.5.2]. Es ist $E|L$ eine endliche Körpererweiterung. Es ist E dann auch ein Zerfällungskörper von $f(X) \in K[X]$, denn das Erzeugnis über K aller Nullstellen von $f(X)$ in E enthält $y_1, \ldots, y_n$, mithin L, stimmt also mit dem Erzeugnis über L aller Nullstellen von $f(X)$ in E überein, welches gleich E ist.

Es ist $E|K$ galoisch; cf. [**5,** §3.5.1.4]. Um zu zeigen, daß der kleinste Teilkörper von E, der $\sigma(L)$ enthält für alle $\sigma \in \mathrm{Gal}(E|K)$, gleich E ist, genügt es zu zeigen, daß für jede Nullstelle $z \in E$ von $f(X)$ ein $\sigma \in \mathrm{Gal}(E|K)$ und ein $i \in [1, n]$ mit $z = \sigma(y_i)$ existiert.

Da $f(z) = 0$ ist, können wir ein $i \in [1,n]$ wählen mit $\mu_{y_i\,,K}(z) = 0$. Also gibt es einen Isomorphismus $\tau : K(y_i) \longrightarrow K(z)$ mit $\tau(y_i) = z$ und $\tau|_K^K = \mathrm{id}_K$; cf. [**5,** §2.3.4]. Es ist E Zerfällungskörper von $f(X) \in K(y_i)[X]$ und auch von $f(X) = f^\tau(X) \in K(z)[X]$. Somit gibt es auch einen Isomorphismus $\sigma : E \longrightarrow E$ mit $\sigma|_{K(y_i)}^{K(z)} = \tau$; cf. [**5,** §2.5.3, Bew. Satz 5]. Für $x \in K$ ist also $\sigma(x) = \tau(x) = x$, i.e. $\sigma|_K^K = \mathrm{id}_K$, i.e. $\sigma \in \mathrm{Gal}(E|K)$. Ferner ist $\sigma(y_i) = \tau(y_i) = z$.

Ad (2). Dank [**5,** §2.5.3, Satz 5] genügt es zu zeigen, daß E ein Zerfällungskörper von $f(X) \in L[X]$ ist; und E' dann ebenfalls. Da $E|K$ galoisch ist und da jeder in $K[X]$ irreduzible Faktor $\mu_{y_i\,,K}(X)$ von $f(X)$ in E die Nullstelle y_i hat für $i \in [1,n]$, zerfällt $f(X) \in E[X]$ in ein Produkt von Linearfaktoren; cf. [**5,** §3.5.1.4]. Ist $\sigma \in \mathrm{Gal}(E|K)$ gegeben, dann ist $\sigma(L) = K(\sigma(y_1)\,,\,\ldots\,,\,\sigma(y_n))$, wobei $f(\sigma(y_i)) = \sigma(f(y_i)) = 0$ ist für $i \in [1,n]$. Da E ein Zerfällungskörper von $L|K$ ist, ist also E über K, und mithin über L, erzeugt von Elementen der Form $\sigma(y_i)$, wobei $\sigma \in \mathrm{Gal}(E|K)$ und $i \in [1,n]$, insbesondere also von Nullstellen von $f(X)$ in E.

Ad (3). Da $F|K$ galoisch ist und da jeder in $K[X]$ irreduzible Faktor $\mu_{y_i\,,K}(X) = \mu^\sigma_{y_i\,,K}(X)$ von $f(X)$ in F die Nullstelle $\sigma(y_i)$ hat für $i \in [1,n]$, zerfällt $f(X)$ in $F[X]$ in ein Produkt von Linearfaktoren; cf. [**5,** §3.5.1.4]. Bezeichnet $L' := \sigma(L)$ und E' das Erzeugnis über K der Nullstellen von $f(X)$ in F, dann ist E' Zerfällungskörper von $f(X) \in K[X]$, enthält $\sigma(y_i)$ stets und ist also auch Zerfällungskörper von $f(X) = f^\sigma(X) \in L'[X]$. Also gibt es einen Isomorphismus $\psi : E \xrightarrow{\sim} E'$ mit $\psi|_L^{L'} = \sigma|^{L'}$; cf. [**5,** §2.5.3]. Sei schließlich φ das Kompositum von ψ mit der Einbettung von E' in F. ▫

> Den Satz vom primitiven Element, daß es ein $y_0 \in L$ mit $L = K(y_0)$ gibt, hätte man im vorstehenden Beweis zur Anwendung bringen können; aber mit einem solchen y_0 will man bei der praktischen Umsetzung nicht unbedingt hantieren müssen; cf. [**5,** Aufgabe 54].

1.2.2 Spur und Norm für endliche Körpererweiterungen

Definition 12 Sei $z \in L$ gegeben.

Betrachte die K-lineare Abbildung

$$\begin{array}{ccc} L & \xrightarrow{\lambda_z} & L \\ y & \longmapsto & zy \end{array}$$

Es ist $\lambda_{uv} = \lambda_u \circ \lambda_v$ für $u,\, v \in L$.

(1) Sei $\mathrm{Tr}_{L|K}(z) := \mathrm{tr}(\lambda_z)$ die *Spur* von z bezüglich $L|K$ (engl. trace).
Das liefert die K-lineare Abbildung $\mathrm{Tr}_{L|K} : L \longrightarrow K$. Es ist $\mathrm{Tr}_{L|K}(1) = [L : K]$.

(2) Sei $\mathrm{N}_{L|K}(z) := \det(\lambda_z)$ die *Norm* von z bezüglich $L|K$.
Das liefert die Abbildung $\mathrm{N}_{L|K} : L \longrightarrow K$ mit $\mathrm{N}_{L|K}(uv) = \mathrm{N}_{L|K}(u)\,\mathrm{N}_{L|K}(v)$ für $u,\, v \in L$ und mit $\mathrm{N}_{L|K}(1) = 1$.

Insbesondere ist $\mathrm{N}_{L|K}(L^\times) \subseteq K^\times$ und $\mathrm{N}_{L|K}\,|_{L^\times}^{K^\times}$ ein Gruppenmorphismus.

Beispiel 13 Betrachte $\mathbf{Q}(\mathrm{i})|\mathbf{Q}$.

Wir verwenden Matrizen bezüglich der $\mathbf{Q}$-linearen Basis $(1, \mathrm{i})$ von $\mathbf{Q}(\mathrm{i})$.

Es ist $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1+3\mathrm{i}) = \mathrm{tr}\left(\begin{smallmatrix}1 & -3\\ 3 & 1\end{smallmatrix}\right) = 2$. Es ist $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1+3\mathrm{i}) = \det\left(\begin{smallmatrix}1 & -3\\ 3 & 1\end{smallmatrix}\right) = 10$. Es ist $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1) = \mathrm{tr}\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) = 2$.

Dahingegen ist $\mathrm{Tr}_{\mathbf{Q}|\mathbf{Q}}(1) = 1$ und $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}(\mathrm{i})}(1+3\mathrm{i}) = 1+3\mathrm{i}$.

Lemma 14

Sei $E|L$ eine endliche Körpererweiterung mit $E|K$ galoisch. Cf. e.g. Lemma 11.(1).

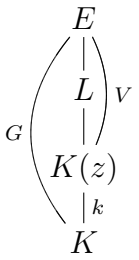
Sei $z \in L$ gegeben. Sei $V := \mathrm{Gal}(E|K(z)) \leqslant \mathrm{Gal}(E|K) =: G$. Sei $k := [K(z) : K]$.

Sei $G = \bigsqcup_{i\in[1,k]} \sigma_i V$, mit $\sigma_i \in G$ für $i \in [1,k]$.

Es ergibt sich für das Minimalpolynom von z über K dann in $E[X]$ die Zerlegung

$$\mu_{z,K}(X) \;=\; \prod_{i\in[1,k]} (X - \sigma_i(z))\;.$$

in ein Produkt von Linearfaktoren.



Beweis. Wir bemerken zunächst, daß das Polynom $\prod_{i\in[1,k]}(X - \sigma_i(z))$ nicht von der Wahl der Repräsentanten σ_i der Elemente in G/V abhängt, da für $\tau \in V$ sich $(\sigma_i \circ \tau)(z) = \sigma_i(z)$ ergibt. Ferner bemerken wir, daß für $\rho \in G$ auch $G = \rho G = \bigsqcup_{i\in[1,k]} \rho\sigma_i V$ ist. Also liefert koeffizientenweise Anwendung von ρ auf $f(X) := \prod_{i\in[1,k]}(X - \sigma_i(z)) \in E[X]$, daß

$$f^\rho(X) \;=\; \prod_{i\in[1,k]} (X - \rho(\sigma_i(z))) \;=\; f(X)$$

ist ; cf. [**5,** §1.6.2]. Somit ist $f(X) \in K[X]$.

Es ist $f(X)$ normiert. Es gibt ein $i \in [1,k]$ mit $\sigma_i \in V$ und also $\sigma_i(z) = z$. Folglich ist $f(z) = 0$. Desweiteren ist $\deg f = k = [K(z) : K]$. Also ist $f(X) = \mu_{z,K}(X)$; cf. [**5,** §2.3.2]. ▫

Lemma 15

Sei $E|L$ eine endliche Körpererweiterung mit $E|K$ galoisch. Cf. e.g. Lemma 11.(1).

Sei $U := \mathrm{Gal}(E|L) \leqslant \mathrm{Gal}(E|K) =: G$, sodaß $L = \mathrm{Fix}_U(E)$ ist; cf. [**5,** §3.5.2].

Schreibe $G = \bigsqcup_{j\in[1,\ell]} \tau_j U$, wobei $\ell := [L : K]$ und $\tau_j \in G$ für $j \in [1, \ell]$.

Es ist $\{ \tau_j|_L \,:\, j \in [1,\ell] \} = \{ \tau|_L \,:\, \tau \in G \}$ eine Menge mit ℓ Elementen.

Falls $E|L$ Zerfällungskörper von $L|K$ ist, dann liegt jeder Körpermorphismus von L nach E, der auf K identisch einschränkt, in dieser Menge.

Gegeben sei $z \in L$.

(1) *Es ist* $\mathrm{Tr}_{L|K}(z) = \sum_{j\in[1,\ell]} \tau_j(z)$.

(2) *Es ist* $\mathrm{N}_{L|K}(z) = \prod_{j\in[1,\ell]} \tau_j(z)$.

Beweis. Für $\tau, \tilde\tau \in G$ ist $\tau|_L = \tilde\tau|_L$ genau dann, wenn $\tilde\tau^{-1}\tau \in U$ ist, i.e. wenn $\tau U = \tilde\tau U$ ist. Daher die behauptete Gleichheit und Kardinalität der Mengen.

Falls $E|L$ Zerfällungskörper von $L|K$ ist, dann kann jeder Körpermorphismus $\sigma : L \longrightarrow E$, für welchen $\sigma|_K^K = \mathrm{id}_K$ ist, gemäß Lemma 11.(3) zu einem Körpermorphismus $\rho : E \longrightarrow E$ fortgesetzt werden, i.e. $\rho|_L = \sigma$. Da ρ wegen $\rho|_K^K = \mathrm{id}_K$ eine K-lineare Abbildung und $[E : K]$ endlich ist, folgt ρ bijektiv und also $\rho \in G$. Also liegt $\sigma = \rho|_L \in \{ \tau|_L \,:\, \tau \in G \}$.

Zunächst merken wir nun die Unabhängigkeit von $\sum_{j\in[1,\ell]} \tau_j(z)$ und $\prod_{j\in[1,\ell]} \tau_j(z)$ von der Wahl der Repräsentanten τ_i der Elemente von G/U an, denn für $\upsilon \in U$ ist $\tau_j\upsilon(z) = \tau_j(z)$ wegen $z \in L$.

Es ist $\deg \mu_{z,K} = [K(z) : K] =: k$. Schreibe $\mu_{z,K}(X) =: \sum_{i\in[0,k]} a_i X^i$.

Schreibe $s := [L : K(z)]$. Dann ist $\ell = [L : K] = [L : K(z)][K(z) : K] = sk$; cf. [**5,** §2.2].

Bezüglich der K-linearen Basis $(z^0, \ldots, z^{k-1})$ von $K(z)$ ist $\lambda_z|_{K(z)}^{K(z)}$ durch die Matrix

$$B \;:=\; \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & \\ & 1 & \ddots & \vdots \\ & & \ddots & 0 \;\; -a_{k-2} \\ & & & 1 \;\; -a_{k-1} \end{pmatrix} \;=\; \sum_{i\in[1,k-1]} \mathrm{e}_{i+1,\,i} - \sum_{i\in[1,k]} a_{i-1}\mathrm{e}_{i,\,k} \;\in\; K^{k\times k}$$

gegeben; cf. [**5,** §2.3.2].

Sei $(y_1, \ldots, y_s)$ eine $K(z)$-lineare Basis von L. Bezüglich der K-linearen Basis $(y_1z^0, \ldots, y_1z^{k-1}, \;\ldots\;, y_sz^0, \ldots, y_sz^{k-1})$ von L ist λ_z durch die Blockdiagonalmatrix

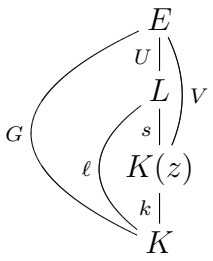
$$C \;:=\; \begin{pmatrix} B & & \\ & \ddots & \\ & & B \end{pmatrix} \;\in\; K^{\ell\times\ell}$$

gegeben; cf. [**5,** §2.2].

Es ist $\mathrm{tr}(B) = -a_{k-1}$ und $\det(B) = (-1)^k a_0$.

Also ist $\mathrm{Tr}_{L|K}(z) = \mathrm{tr}(C) = s \cdot \mathrm{tr}(B) = -sa_{k-1}$ und $\mathrm{N}_{L|K}(z) = (\det(B))^s = (-1)^\ell a_0^s$.

Sei $V := \mathrm{Gal}(E|K(z))$. Es ist $U \leqslant V \leqslant G$.



Sei $G = \bigsqcup_{i\in[1,k]} \sigma_i V$, mit $\sigma_i \in G$ für $i \in [1,k]$. Dank Lemma 14 ist

$$\sum_{i\in[0,k]} a_i X^i \;=\; \mu_{z,K}(X) \;=\; \prod_{i\in[1,k]} (X - \sigma_i(z))\;,$$

und also $a_{k-1} = -\sum_{i\in[1,k]} \sigma_i(z)$ und $a_0 = (-1)^k \prod_{i\in[1,k]} \sigma_i(z)$.

Schreibe $V = \bigsqcup_{t\in[1,s]} \rho_t U$ mit $\rho_t \in V$ für $t \in [1,s]$. Dann ist auch $G = \bigsqcup_{i\in[1,k]} \sigma_i V = \bigsqcup_{i\in[1,k]} \bigsqcup_{t\in[1,s]} \sigma_i\rho_t U$. Wegen der Unabhängigkeit von der Wahl der Repräsentanten von G/U erhalten wir

$$\sum_{j\in[1,\ell]} \tau_j(z) \;=\; \sum_{i\in[1,k]} \sum_{t\in[1,s]} \sigma_i\rho_t(z) \;=\; \sum_{i\in[1,k]} \sum_{t\in[1,s]} \sigma_i(z) \;=\; s\cdot \sum_{i\in[1,k]} \sigma_i(z) \;=\; -sa_{k-1} \;=\; \mathrm{Tr}_{L|K}(z)$$

und

$$\prod_{j\in[1,\ell]} \tau_j(z) \;=\; \prod_{i\in[1,k]} \prod_{t\in[1,s]} \sigma_i\rho_t(z) \;=\; \prod_{i\in[1,k]} \prod_{t\in[1,s]} \sigma_i(z) \;=\; (\prod_{i\in[1,k]} \sigma_i(z))^s \;=\; (-1)^\ell a_0^s \;=\; \mathrm{N}_{L|K}(z)\;.$$

□

Korollar 16 *Ist $L|K$ galoisch, so gilt für $z \in L$ folgendes.*

(1) *Es ist* $\mathrm{Tr}_{L|K}(z) = \sum_{\tau\in\mathrm{Gal}(L|K)} \tau(z)$.

(2) *Es ist* $\mathrm{N}_{L|K}(z) = \prod_{\tau\in\mathrm{Gal}(L|K)} \tau(z)$.

Beweis. In den Bezeichnungen von Lemma 15 sei $E := L$. Dann ist $G = \mathrm{Gal}(L|K)$ und $U = \mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$, sodaß die Repräsentanten von G/U ganz G durchlaufen, i.e. $\{\,\tau_j : j \in [1,\ell]\,\} = G$. Die beiden Formeln folgen nun aus Lemma 15. □

Beispiel 17 Es ist $\mathrm{Gal}(\mathbf{Q}(\mathrm{i})|\mathbf{Q}) = \{\,\mathrm{id}_{\mathbf{Q}(\mathrm{i})}\,,\,\sigma\,\}$, wobei $\sigma : \mathbf{Q}(\mathrm{i}) \longrightarrow \mathbf{Q}(\mathrm{i})$, $\mathrm{i} \longmapsto -\mathrm{i}$.

Es ist $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1{+}3\mathrm{i}) = \mathrm{id}_{\mathbf{Q}(\mathrm{i})}(1{+}3\mathrm{i}){+}\sigma(1{+}3\mathrm{i}) = (1{+}3\mathrm{i}){+}(1{-}3\mathrm{i}) = 2$ und $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1{+}3\mathrm{i}) = (1+3\mathrm{i})(1-3\mathrm{i}) = 10$. Cf. Beispiel 13.

Lemma 18 *Es ist die Spur* $\mathrm{Tr}_{L|K} : L \longrightarrow K$ *nicht die Nullabbildung.*

Beweis. Sei E ein Zerfällungskörper von $L|K$; cf. Lemma 11.(1, 2). Wir verwenden die Bezeichnungen aus Lemma 15. Für $i, j \in [1, \ell]$ mit $i \neq j$ ist $\tau_i U \neq \tau_j U$ und also $\tau_i|_L \neq \tau_j|_L$. Somit ist das Tupel $(\tau_1|_L, \ldots, \tau_\ell|_L)$ linear unabhängig über E; cf. **[5,** §3.5.1.1]. Insbesondere ist $\mathrm{Tr}_{L|K} = (\sum_{i\in[1,\ell]} \tau_i|_L)|^K \neq 0$. ▫

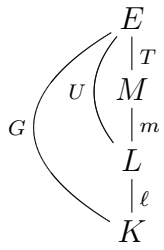
Lemma 19 *Seien* $M|L|K$ *Körpererweiterungen.*

(1) *Es ist* $\mathrm{Tr}_{M|K} = \mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L}$.

(2) *Es ist* $\mathrm{N}_{M|K} = \mathrm{N}_{L|K} \circ \mathrm{N}_{M|L}$.

Beweis. Sei E ein Zerfällungskörper von $M|K$; cf. Lemma 11.(1, 2).

Sei $T := \mathrm{Gal}(E|M) \leqslant U := \mathrm{Gal}(E|L) \leqslant \mathrm{Gal}(E|K) =: G$, sodaß $M = \mathrm{Fix}_T(E)$ und $L = \mathrm{Fix}_U(E)$ ist; cf. **[5,** §3.5.2].



Sei $G = \bigsqcup_{i\in[1,\ell]} \tau_i U$, wobei $\ell = [L : K]$ und $\tau_i \in G$ für $i \in [1, \ell]$.

Sei $U = \bigsqcup_{j\in[1,m]} \rho_j T$, wobei $m = [M : L]$ und $\rho_j \in U$ für $j \in [1, m]$.

Dann ist $G = \bigsqcup_{i\in[1,\ell]} \tau_i U = \bigsqcup_{i\in[1,\ell]} \bigsqcup_{j\in[1,m]} \tau_i \rho_j T$.

Sei $z \in M$ gegeben.

Mit dreifacher Anwendung von Lemma 15.(1) wird

$$\begin{aligned}(\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L})(z) &= \mathrm{Tr}_{L|K}\big(\textstyle\sum_{j\in[1,m]} \rho_j(z)\big) = \sum_{i\in[1,\ell]} \tau_i\big(\sum_{j\in[1,m]} \rho_j(z)\big) \\ &= \textstyle\sum_{i\in[1,\ell]} \sum_{j\in[1,m]} \tau_i\rho_j(z) = \mathrm{Tr}_{M|K}(z)\,.\end{aligned}$$

Mit dreifacher Anwendung von Lemma 15.(2) wird

$$\begin{aligned}(\mathrm{N}_{L|K} \circ \mathrm{N}_{M|L})(z) &= \mathrm{N}_{L|K}\big(\textstyle\prod_{j\in[1,m]} \rho_j(z)\big) = \prod_{i\in[1,\ell]} \tau_i\big(\prod_{j\in[1,m]} \rho_j(z)\big) \\ &= \textstyle\prod_{i\in[1,\ell]} \prod_{j\in[1,m]} \tau_i\rho_j(z) = \mathrm{N}_{M|K}(z)\,.\end{aligned}$$

▫

1.3 Der Ring der ganzen Elemente in einer endlichen Körpererweiterung

Sei K ein perfekter Körper.

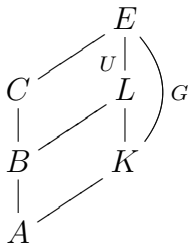
Sei $L|K$ eine endliche Körpererweiterung. Schreibe $\ell := [L : K]$.

Sei $E|L$ eine endliche Körpererweiterung mit $E|K$ galoisch. Cf. auch Definition 9, Lemma 11.(1). Sei

$$U \;:=\; \mathrm{Gal}(E|L) \;\leqslant\; \mathrm{Gal}(E|K) \;=:\; G\,.$$

Sei $G = \bigsqcup_{j\in[1,\ell]} \tau_j U$ mit $\tau_j \in G$ für $j \in [1,\ell]$. Sei dabei o.E. $\tau_1 := \mathrm{id}_E$.

Sei $A \subseteq K$ ein ganzabgeschlossener Teilring mit $K = \mathrm{Quot}(A)$. Sei $B := \Gamma_L(A)$. Sei $C := \Gamma_E(A)$.



Dann ist auch $C = \Gamma_E(B)$; cf. Aufgabe 5.(2). Es sind A, B und C ganzabgeschlossen; cf. Bemerkung 8.(2).

Falls bereits $L|K$ galoisch ist, dann ist $E := L$ wählbar, was $C = B$ nach sich zieht.

1.3.1 Spur und Norm und ganze Elemente

Lemma 20

(1) *Es ist* $\rho(C) = C$ *für* $\rho \in G$.

(2) *Es ist* $\mathrm{Tr}_{L|K}(B) \subseteq A$.

(3) *Es ist* $\mathrm{N}_{L|K}(B) \subseteq A$.

(4) *Für* $b \in B$ *liegt genau dann* $b \in \mathrm{U}(B)$, *wenn* $\mathrm{N}_{L|K}(b) \in \mathrm{U}(A)$ *liegt.*

Cf. auch Aufgabe 12.

Beweis.

Ad (1). Es genügt, $\rho(C) \overset{!}{\subseteq} C$ zu zeigen; die umgekehrte Inklusion folgt dann unter Verwendung von $\rho^{-1} \in G$.

Seien $\rho \in G$ und $c \in C$ gegeben. Es ist $\rho(c) \overset{!}{\in} C$ zu zeigen.

Es gibt $f(X) \in A[X]$ normiert mit $f(c) = 0$. Also ist auch $f(\rho(c)) = \rho(f(c)) = 0$ und somit $\rho(c) \in C$.

Ad (2). Sei $b \in B$ gegeben. Es ist $\mathrm{Tr}_{L|K}(b) = \sum_{j\in[1,\ell]} \tau_j(b)$; cf. Lemma 15.(1). Dank (1) ist darin jeder Summand $\tau_j(b) \in C$ und also auch deren Summe $\mathrm{Tr}_{L|K}(b) \in C$. Auf der anderen Seite ist $\mathrm{Tr}_{L|K}(b) \in K$. Also ist

$$\mathrm{Tr}_{L|K}(b) \;\in\; C \cap K \;=\; \Gamma_E(A) \cap K \;=\; \Gamma_K(A) \;=\; A\,,$$

da A ganzabgeschlossen ist.

Ad (3). Wir verwenden das Argument aus (2), in welchem überall die Summe durch das Produkt ersetzt wird.

Ad (4).

Sei zum einen $b \in \mathrm{U}(B)$. Dann ist sowohl $\mathrm{N}_{L|K}(b)$ als auch $\mathrm{N}_{L|K}(b^{-1})$ in A ; cf. (3). Es wird $\mathrm{N}_{L|K}(b)\,\mathrm{N}_{L|K}(b^{-1}) = \mathrm{N}_{L|K}(bb^{-1}) = \mathrm{N}_{L|K}(1) = 1$. Also ist $\mathrm{N}_{L|K}(b) \in \mathrm{U}(A)$.

Sei zum anderen $\mathrm{N}_{L|K}(b) \in \mathrm{U}(A)$. Schreibe $a := \mathrm{N}_{L|K}(b)^{-1} \in A$. Es ist $b \in B^\times$.

Es ist

$$1 \;=\; a\,\mathrm{N}_{L|K}(b) \;=\; a \cdot \prod_{j\in[1,\ell]} \tau_j(b) \;=\; b \cdot \underbrace{\big(a \cdot \prod_{j\in[2,\ell]} \tau_j(b)\big)}_{=:\,c}\,.$$

Dank (1) ist $c \in C$. In E gerechnet ist $c = b^{-1}$. Da $b \in L$, liegt auch $b^{-1} \in L$. Es ist also $c \in C \cap L = \Gamma_E(A) \cap L = \Gamma_L(A) = B$. Folglich ist $b \in \mathrm{U}(B)$. ▫

Beispiel 21

(1) Sei $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = E = \mathbf{Q}(\mathrm{i})$. Dann ist $B = C = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3 oder 6.
Für $x,\, y \in \mathbf{Z}$ ist $x + \mathrm{i}y$ genau dann in $\mathrm{U}(\mathbf{Z}[\mathrm{i}])$, wenn

$$\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(x + \mathrm{i}y) \;=\; (x + \mathrm{i}y)(x - \mathrm{i}y) \;=\; x^2 + y^2 \;\in\; \mathrm{U}(\mathbf{Z}) \;=\; \{-1, +1\}$$

liegt, i.e. wenn $x + \mathrm{i}y \in \{-1, +1, -\mathrm{i}, +\mathrm{i}\}$ liegt; cf. Korollar 16.(2). Somit ist

$$\mathrm{U}(\mathbf{Z}[\mathrm{i}]) \;=\; \langle \mathrm{i} \rangle \;\simeq\; \mathrm{C}_4\,.$$

(2) Sei $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = E = \mathbf{Q}(\sqrt{-5})$. Dann ist $B = C = \mathbf{Z}[\sqrt{-5}]$; cf. Aufgabe 3.
Für $x,\, y \in \mathbf{Z}$ ist $x + y\sqrt{-5}$ genau dann in $\mathrm{U}(\mathbf{Z}[\sqrt{-5}])$, wenn

$$\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x+y\sqrt{-5}) \;=\; (x+y\sqrt{-5})(x-y\sqrt{-5}) \;=\; x^2+5y^2 \;\in\; \mathrm{U}(\mathbf{Z}) \;=\; \{-1, +1\}$$

liegt, wenn also $y = 0$ ist und $x \in \{-1, +1\}$ liegt. Somit ist

$$\mathrm{U}(\mathbf{Z}[\sqrt{-5}]) \;=\; \langle -1 \rangle \;\simeq\; \mathrm{C}_2\,.$$

1.3.2 Diskriminante

Sei $\underline{y} := (y_1 , y_2 , \ldots , y_\ell)$ eine K-lineare Basis von L.

Lemma 22 *Betrachte die K-Bilinearform*

$$\begin{array}{ccccc} L & \times & L & \longrightarrow & K \\ (x & , & y) & \longmapsto & \mathrm{Tr}_{L|K}(xy) \ , \end{array}$$

genannt Spurbilinearform *auf L über K.*

Sie ist nichtausgeartet.

Ihre Grammatrix $\mathrm{Gram}_{L|K,\,\underline{y}} := (\mathrm{Tr}_{L|K}(y_i y_j))_{i,\,j} \in K^{\ell\times\ell}$ *ist daher invertierbar.*

Folglich liegt die Diskriminante *von $L|K$ bezüglich der K-linearen Basis $\underline{y}$, welche als*

$$\Delta_{L|K,\,\underline{y}} \ := \ \det(\mathrm{Gram}_{L|K,\,\underline{y}})$$

definiert ist, in $K^\times$.

Beweis. Sei $x \in L^\times$ gegeben. Wir müssen ein $y \in L$ mit $\mathrm{Tr}_{L|K}(xy) \neq 0$ finden.

Es ist $\mathrm{Tr}_{L|K}$ nicht die Nullabbildung; cf. Lemma 18. Also können wir ein $z \in L$ mit $\mathrm{Tr}_{L|K}(z) \neq 0$ wählen. Mit $y := x^{-1}z$ wird dann $\mathrm{Tr}_{L|K}(xy) = \mathrm{Tr}_{L|K}(z) \neq 0$. ▫

Beispiel 23 Wir betrachten $\mathbf{Q}(\mathrm{i})|\mathbf{Q}$ und die $\mathbf{Q}$-lineare Basis $(1, \mathrm{i})$ von $\mathbf{Q}(\mathrm{i})$. Wir erhalten

$$\Delta_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,(1,\mathrm{i})} \ = \ \det\begin{pmatrix} \mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1\cdot 1) & \mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1\cdot \mathrm{i}) \\ \mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\mathrm{i}\cdot 1) & \mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\mathrm{i}\cdot \mathrm{i}) \end{pmatrix} \ = \ \det\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \ = \ -4 \ .$$

Lemma 24 *Sei*

$$\mathrm{Vand}_{L|K,\,\underline{y}} \ := \ (\tau_j(y_i))_{i,\,j} \ \in \ E^{\ell\times\ell}$$

die (verallgemeinerte) Vandermondematrix.

Dann ist

$$\begin{array}{rcl} \mathrm{Gram}_{L|K,\,\underline{y}} & = & \mathrm{Vand}_{L|K,\,\underline{y}}\,\mathrm{Vand}^{\mathrm{t}}_{L|K,\,\underline{y}} \\ \Delta_{L|K,\,\underline{y}} & = & \det(\mathrm{Vand}_{L|K,\,\underline{y}})^2 \ . \end{array}$$

Beachte noch, daß $\mathrm{Vand}_{L|K,\,\underline{y}}$ auch von der Wahl von E abhängt und daß ihre Spaltenreihenfolge von der Numerierung der Repräsentanten τ_j abhängt.

Beweis. Wir haben nur erste Gleichung zu zeigen.

Der Eintrag an Position $(i, j) \in [1, \ell] \times [1, \ell]$ des Matrixproduktes der rechten Seite ist

$$\sum_{k\in[1,\ell]} \tau_k(y_i)\tau_k(y_j) \ = \ \sum_{k\in[1,\ell]} \tau_k(y_i y_j) \ \overset{\text{L. 15.(1)}}{=} \ \mathrm{Tr}_{L|K}(y_i y_j) \ ,$$

und das ist der Eintrag von $\mathrm{Gram}_{L|K,\,\underline{y}}$ an Position (i, j). ▫

Bemerkung 25 Sei ein Element $z \in L$ mit $L = K(z)$ gefunden. Wir haben die K-lineare Basis $(z^i \,:\, i \in [0, \ell-1]) = (z^0, z^1, \ldots, z^{\ell-1})$ von L. Dann ist

$$\mathrm{Vand}_{L|K,\,(\,z^i\,:\,i\,\in\,[0,\ell-1]\,)} \;=\; (\tau_j(z^{i-1}))_{i,\,j} \;=\; (\tau_j(z)^{i-1})_{i,\,j} \;\in\; E^{\ell\times\ell}$$

eine Vandermondematrix im klassischen Sinn. Ihre Determinante ergibt sich mit Induktion und Spalten- und Zeilenvereinfachungen zu

$$\det(\mathrm{Vand}_{L|K,\,(\,z^i\,:\,i\,\in\,[0,\ell-1]\,)}) \;=\; \prod_{1\leqslant i<j\leqslant\ell} (\tau_j(z) - \tau_i(z)) \;.$$

Gemäß Lemma 24 ist folglich

$$\Delta_{L|K,\,(\,z^i\,:\,i\,\in\,[0,\ell-1]\,)} \;=\; \prod_{1\leqslant i<j\leqslant\ell} (\tau_j(z) - \tau_i(z))^2 \;.$$

Beispiel 26

(1) Wir setzen die Beispiele 17 und 23 fort. Schreibe $\underline{y} = (1, \mathrm{i})$.

Es ist $\mathrm{Vand}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,\underline{y}} = \left(\begin{smallmatrix} 1 & 1 \\ \mathrm{i} & -\mathrm{i} \end{smallmatrix}\right)$.

Mit Bemerkung 25 (oder mittels direkter Berechnung) wird nun

$$\det(\mathrm{Vand}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,(1,\mathrm{i})}) \;=\; \sigma(\mathrm{i}) - \mathrm{id}_{\mathbf{Q}(\mathrm{i})}(\mathrm{i}) \;=\; (-\mathrm{i}) - \mathrm{i} \;=\; -2\mathrm{i} \;.$$

Folglich wird erneut $\Delta_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,(1,\mathrm{i})} = (-2\mathrm{i})^2 = -4$.

(2) Sei $K = \mathbf{Q}$, $\delta := \sqrt[3]{2}$, $\zeta := \zeta_3$, $L = \mathbf{Q}(\delta)$, $E = \mathbf{Q}(\delta, \zeta)$; cf. Aufgabe 7. Die Elemente von $\mathrm{Gal}(\mathbf{Q}(\delta,\zeta)|\mathbf{Q})$ schränken auf $\mathbf{Q}(\delta)$ so ein, daß δ auf δ resp. auf $\zeta\delta$ resp. auf $\zeta^2\delta$ abgebildet wird. Mit Bemerkung 25 wird

$$\det(\mathrm{Vand}_{\mathbf{Q}(\delta)|\mathbf{Q},\,(1,\delta,\delta^2)}) \;=\; (\zeta\delta-\delta)(\zeta^2\delta-\delta)(\zeta^2\delta-\zeta\delta) \;=\; \delta^3 \underbrace{(\zeta-1)(\zeta^2-1)}_{=\,3} \underbrace{(\zeta^2-\zeta)}_{-\mathrm{i}\sqrt{3}} \;=\; -6\mathrm{i}\sqrt{3} \;.$$

Somit ist

$$\Delta_{\mathbf{Q}(\delta)|\mathbf{Q},\,(1,\delta,\delta^2)} \;=\; (-6\mathrm{i}\sqrt{3})^2 = -2^2\cdot 3^3 \;.$$

Alternativ dazu können wir auch $\mathrm{Tr} := \mathrm{Tr}_{\mathbf{Q}(\delta)|\mathbf{Q}}$ schreiben,

$$\mathrm{Tr}(\delta^k) \;\overset{\text{L. 15.(1)}}{=}\; \delta^k + (\zeta\delta)^k + (\zeta^2\delta)^k \;=\; 3\partial_{k+3\mathbf{Z},\,0+3\mathbf{Z}}\delta^k$$

für $k \geqslant 0$ bestimmen und somit

$$\Delta_{\mathbf{Q}(\delta)|\mathbf{Q},\,(1,\delta,\delta^2)} \;=\; \det(\mathrm{Gram}_{\mathbf{Q}(\delta)|\mathbf{Q},\,(1,\delta,\delta^2)}) \;=\; \det\begin{pmatrix} \mathrm{Tr}(1\cdot1) & \mathrm{Tr}(1\cdot\delta) & \mathrm{Tr}(1\cdot\delta^2) \\ \mathrm{Tr}(\delta\cdot1) & \mathrm{Tr}(\delta\cdot\delta) & \mathrm{Tr}(\delta\cdot\delta^2) \\ \mathrm{Tr}(\delta^2\cdot1) & \mathrm{Tr}(\delta^2\cdot\delta) & \mathrm{Tr}(\delta^2\cdot\delta^2) \end{pmatrix} \;=\; \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3\cdot2 \\ 0 & 3\cdot2 & 0 \end{pmatrix} \;=\; -2^2\cdot3^3$$

berechnen.

1.3.3 Basen

Lemma 27 *Für alle $y \in L$ gibt es ein $a \in A^\times$ mit $ay \in B$.*

Beweis. Sei $\mu_{y,K}(X) =: X^n + \sum_{i\in[0,n-1]} s_i X^i \in K[X]$, wobei $n := \deg(\mu_{y,K})$. Da $K = \mathrm{Quot}(A)$, gibt es ein $a \in A^\times$ mit $as_i \in A$ für $i \in [0, n-1]$. Es wird

$$0 \;=\; a^n(y^n + \sum_{i\in[0,n-1]} s_i y^i) \;=\; (ay)^n + \sum_{i\in[0,n-1]} \underbrace{a^{n-i}s_i}_{\in A}(ay)^i \;,$$

und damit ist $ay \in \Gamma_A(L) = B$. □

Lemma 28 *Es gibt eine K-lineare Basis von L, deren Elemente in B liegen.*

Beweis. Sei $(\, y_i \,:\, i \in [1,\ell]\,)$ eine K-lineare Basis von L. Dank Lemma 27 gibt es ein $a \in A^\times$ mit $ay_i \in B$ für alle $i \in [1,\ell]$. Da $\lambda_a : L \longrightarrow L$, $z \longmapsto az$ eine bijektive K-lineare Abbildung ist, ist $(\, ay_i \,:\, i \in [1,\ell]\,)$ eine K-lineare Basis von L, deren Elemente in B liegen. □

Definition 29 Sei $M \subseteq L$ ein A-Teilmodul. Sei

$$M^{\#,A} \;:=\; \{\, x \in L \,:\, \mathrm{Tr}_{L|K}(xM) \subseteq A \,\}$$

sein *Dual*. Wir schreiben oft $M^\# := M^{\#,A}$, wenn A aus dem Kontext hervorgeht.

Bemerkung 30 *Es ist $B \subseteq B^\#$.*

Beweis. Für $b \in B$ ist $\mathrm{Tr}_{L|K}(bB) \subseteq \mathrm{Tr}_{L|K}(B) \subseteq A$ gemäß Lemma 20.(2). □

Lemma 31

(1) *Sei $M \subseteq L$ ein A-Teilmodul. Es ist $M^\# \subseteq L$ ein A-Teilmodul.*

(2) *Sind $M \subseteq N \subseteq L$ zwei A-Teilmoduln, dann ist $N^\# \subseteq M^\# \subseteq L$.*

(3) *Sei $(\, y_i \,:\, i \in [1,\ell]\,)$ eine K-lineare Basis von L. Sei $(\, y_i' \,:\, i \in [1,\ell]\,)$ die dazu bezüglich der Spurbilinearform von $L|K$ duale Basis, i.e. es sei $\mathrm{Tr}_{L|K}(y_i y_j') = \partial_{i,j}$ für $i,\, j \in [1,\ell]$; cf. Lemma 22.*

Ist $M = {}_A\langle\, y_i \,:\, i \in [1,\ell]\,\rangle$, dann ist $M^\# = {}_A\langle\, y_i' \,:\, i \in [1,\ell]\,\rangle$.

Insbesondere ist dann $M^{\#\#} = M$.

Beweis.

Ad (1). Es ist $0 \in M^{\#}$.

Seien $x, x' \in M^{\#}$ und $a, a' \in A$. Zu zeigen ist $ax + a'x' \overset{!}{\in} M^{\#}$. Sei $m \in M$ gegeben. Zu zeigen ist $\mathrm{Tr}_{L|K}((ax + a'x')m) \overset{!}{\in} A$. In der Tat ist $\mathrm{Tr}_{L|K}((ax + a'x')m) = a\underbrace{\mathrm{Tr}_{L|K}(xm)}_{\in A} + a'\underbrace{\mathrm{Tr}_{L|K}(x'm)}_{\in A} \in A$.

Ad (2). Ist $x \in N^{\#}$, dann ist $\mathrm{Tr}_{L|K}(xM) \subseteq \mathrm{Tr}_{L|K}(xN) \subseteq A$, also $x \in M^{\#}$.

Ad (3). Sei $z \in L$ gegeben. Schreibe $z = \sum_{j\in[1,\ell]} s_j y'_j$ mit $s_i \in K$.

Es ist $z \in M^{\#}$ genau dann, wenn

$$\mathrm{Tr}_{L|K}(zy_i) \;=\; \sum_{j\in[1,\ell]} s_j \,\mathrm{Tr}_{L|K}(y'_j y_i) \;=\; \sum_{j\in[1,\ell]} s_j \partial_{i,\,j} \;=\; s_i$$

in A liegt für $i \in [1,\ell]$, i.e. wenn $z \in {}_A\langle\, y'_i \,:\, i \in [1,\ell]\,\rangle$ liegt. ▫

Beispiel 32

(1) Betrachte $\mathbf{Q}(\mathrm{i})|\mathbf{Q}$. Schreibe $\mathrm{Tr} := \mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}$. Es ist $\mathcal{O}_{\mathbf{Q}(\mathrm{i})} = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Wir wollen $\mathcal{O}^{\#}_{\mathbf{Q}(\mathrm{i})}$ berechnen. Ist $\underline{y} = (1, \mathrm{i})$, so wird $\mathcal{O}_{\mathbf{Q}(\mathrm{i})} = {}_{\mathbf{Z}}\langle \underline{y} \rangle$. Wir haben die zugehörige Dualbasis $\underline{y'}$ zu berechnen, denn dann wird $\mathcal{O}^{\#}_{\mathbf{Q}(\mathrm{i})} = {}_{\mathbf{Z}}\langle \underline{y'} \rangle$; cf. Lemma 31.(3).
Es ist

$$\begin{pmatrix} \mathrm{Tr}((a+b\mathrm{i})\cdot 1) & \mathrm{Tr}((a+b\mathrm{i})\cdot \mathrm{i}) \end{pmatrix} \;=\; \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot \mathrm{i}) \\ \mathrm{Tr}(\mathrm{i}\cdot 1) & \mathrm{Tr}(\mathrm{i}\cdot \mathrm{i}) \end{pmatrix} \;=\; \begin{pmatrix} a & b \end{pmatrix} \mathrm{Gram}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,(1,\mathrm{i})}$$

für $a, b \in \mathbf{Q}$. Da die Elemente von $\underline{y'}$ hier $\begin{pmatrix} 1 & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & 1 \end{pmatrix}$ liefern sollen, stehen ihre Koeffizienten in den Zeilen der Inversen $(\mathrm{Gram}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q},\,(1,\mathrm{i})})^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Somit wird $\underline{y'} = (\,\frac{1}{2}\,,\, -\frac{1}{2}\mathrm{i}\,)$ und also

$$\mathcal{O}^{\#}_{\mathbf{Q}(\mathrm{i})} = {}_{\mathbf{Z}}\langle\, \tfrac{1}{2}\,,\, -\tfrac{1}{2}\mathrm{i}\,\rangle\,.$$

(2) Betrachte $\mathbf{Q}(\sqrt{5})|\mathbf{Q}$. Schreibe $\alpha := \frac{1+\sqrt{5}}{2}$ und $\mathrm{Tr} := \mathrm{Tr}_{\mathbf{Q}(\alpha)|\mathbf{Q}}$. Es ist $\alpha^2 = \alpha + 1$. Es ist $\mathrm{Tr}(\alpha) = \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = 1$. Also ist $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha + 1) = 3$.
Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\alpha] = {}_{\mathbf{Z}}\langle 1, \alpha \rangle$; cf. Aufgabe 3. Es ist

$$(\mathrm{Gram}_{\mathbf{Q}(\alpha)|\mathbf{Q},\,(1,\alpha)})^{-1} \;=\; \begin{pmatrix} \mathrm{Tr}(1\cdot 1) & \mathrm{Tr}(1\cdot \alpha) \\ \mathrm{Tr}(\alpha\cdot 1) & \mathrm{Tr}(\alpha\cdot \alpha) \end{pmatrix}^{-1} \;=\; \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}^{-1} = \frac{1}{5}\begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix}\,.$$

Folglich ist die zu $(1, \alpha)$ duale Basis gegeben durch $(\frac{1}{5}(3-\alpha),\, \frac{1}{5}(-1+2\alpha))$. Somit ist

$$\mathcal{O}^{\#}_{\mathbf{Q}(\sqrt{5})} \;=\; {}_{\mathbf{Z}}\langle\, \tfrac{1}{5}(3-\alpha)\,,\, \tfrac{1}{5}(-1+2\alpha)\,\rangle\,.$$

Lemma 33 (Existenz einer A-linearen Basis)

Sei $\underline{g}$ ein endliches Tupel von Elementen von L. Die folgenden Aussagen $(1, 2)$ sind äquivalent.

(1) *Es ist $\underline{g}$ eine A-lineare Basis von B.*

(2) *Es ist $\underline{g}$ eine K-lineare Basis von L mit $B = {}_A\langle \underline{g} \rangle$.*

Insbesondere besteht jede A-lineare Basis von B aus ℓ Elementen.

Ist A ein Hauptidealbereich, dann gibt es eine A-lineare Basis von B.

Ist $A = \mathbf{Z}$ und $B = \mathcal{O}_L$, so heißt eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_L$ auch Ganzheitsbasis.

Beweis.

Ad (2) $\Longrightarrow$ (1). Da $\underline{g}$ ein K-linear unabhängiges Tupel ist, ist es auch A-linear unabhängig.

Ad (1) $\Longrightarrow$ (2). Da $\underline{g}$ ein A-linear unabhängiges Tupel ist, ist es auch K-linear unabhängig. Denn *gäbe* es eine nichttriviale K-Linearkombination von $\underline{g}$, die 0 ergibt, so könnten wir diese mit einem gemeinsamen Nenner der Koeffizienten multiplizieren und erhielten eine nichttriviale K-Linearkombination von $\underline{g}$, die 0 ergibt, welche es aber *nicht* gibt. Bleibt zu zeigen, daß ${}_K\langle \underline{g} \rangle = L$ ist. Sei $y \in L$ gegeben. Schreibe $y = a^{-1}b$ für ein $a \in A^\times$ und ein $b \in B$; cf. Lemma 27. Dann ist $b \in B = {}_A\langle \underline{g} \rangle \subseteq {}_K\langle \underline{g} \rangle$ und also auch $y = a^{-1}b \in {}_K\langle \underline{g} \rangle$.

Sei nun A als Hauptidealbereich vorausgesetzt. Wir wollen zeigen, daß es eine A-lineare Basis von B gibt.

Sei $(\, y_i \,:\, i \in [1, \ell]\,)$ eine K-lineare Basis von L, die in B liegt; cf. Lemma 28. Sei $M := {}_A\langle\, y_i \,:\, i \in [1, \ell]\,\rangle$. Es hat $M^\#$ eine A-lineare Basis aus ℓ Elementen; cf. Lemma 31.(3). Es ist

$$M \;\subseteq\; B \overset{\text{B.30}}{\subseteq} B^\# \overset{\text{L. 31.(2)}}{\subseteq} M^\# \,.$$

Da A ein Hauptidealbereich ist, folgt aus $M^\#$ endlich erzeugt frei über A auch B endlich erzeugt frei über A; cf. Aufgabe 13.(2). Mit anderen Worten, es gibt eine A-lineare Basis von B. ▫

> Auch aus $M \subseteq B \subseteq M^\#$ folgt übrigens $\ell = \mathrm{rk}_A(M) \leqslant \mathrm{rk}_A(B) \leqslant \mathrm{rk}_A(M^\#) = \ell$; cf. Aufgabe 13.(2).

Bemerkung 34 *Sei $\underline{y} = (\, y_i \,:\, i \in [1, \ell]\,)$ ein Tupel von Elementen von B. Genau dann ist die A-lineare Abbildung $\varphi : A^{\oplus \ell} \longrightarrow B$, $(a_i)_{i \in [1,\ell]} \longmapsto \sum_{i \in [1,\ell]} a_i y_i$ bijektiv, wenn $\underline{y}$ eine A-lineare Basis von B ist.*

Beweis.

Ad $\Rightarrow$. Da φ surjektiv ist, ist $B = {}_A\langle \underline{y} \rangle$.

Wir haben zu zeigen, daß $\underline{y}$ eine K-lineare Basis von L ist. Aus Dimensionsgründen genügt es, die K-lineare Unabhängigkeit von $\underline{y}$ zu zeigen..

Sei $\sum_{i\in[1,\ell]} x_i y_i = 0$ mit $x_i \in K$ für $i \in [1,\ell]$ gegeben. Wähle $c \in A^\times$ mit $cx_i \in A$ für $i \in [1,\ell]$. Dann ist $\varphi((cx_i)_{i\in[1,\ell]}) = c(\sum_{i\in[1,\ell]} x_i y_i) = 0$, wegen der Injektivität von φ somit $cx_i = 0$ und also $x_i = 0$ für $i \in [1,\ell]$.

Ad $\Leftarrow$. Die Surjektivität von φ folgt aus $B = {}_A\langle \underline{y}\rangle$. Die Injektivität von φ folgt aus der K-linearen Unabhängigkeit von $\underline{y}$ durch Anwendung auf Linearkombinationen mit Koeffizienten in $A \subseteq K$. ▫

Beispiel 35

(1) Betrachte $\mathbf{Q}(\mathrm{i})|\mathbf{Q}$. Eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\mathrm{i})}$ ist $(1, \mathrm{i})$; cf. Aufgabe 3.

(2) Betrachte $\mathbf{Q}(\sqrt{5})|\mathbf{Q}$. Eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\sqrt{5})}$ ist $(1, \frac{1+\sqrt{5}}{2})$; cf. Aufgabe 3.

Lemma 36 (Eindeutigkeit der Diskriminate bis auf Einheitenquadrat)

Ist A ein Hauptidealbereich und $\underline{g} := (\, g_i \,:\, i \in [1,\ell]\,)$ eine A-lineare Basis von B, so heißt

$$\Delta_{L|K,\,\underline{g}} \;\in\; A$$

auch die Diskriminante von $B|A$ *bezüglich* $\underline{g}$.

Sind mit $\underline{g} := (\, g_i \,:\, i \in [1,\ell]\,)$ und $\underline{h} := (\, h_i \,:\, i \in [1,\ell]\,)$ uns A-lineare Basen von B gegeben, so gibt es ein Element $e \in \mathrm{U}(A)$ mit

$$\Delta_{L|K,\,\underline{g}} \;=\; e^2 \Delta_{L|K,\,\underline{h}}$$

Mit anderen Worten, bis auf das Quadrat einer Einheit in A liegt die Diskriminante von $B|A$ eindeutig fest.

Beweis. Es ist $\Delta_{L|K,\,\underline{g}} \in A$, da $\mathrm{Tr}_{L|K}(g_i g_j) \in A$ für $i,\, j \,\in\, [1,\ell]$; cf. Lemmata 20.(2) und 22. Schreibe $g_i = \sum_{j\in[1,\ell]} a_{j,i} h_j$ und $h_j = \sum_{k\in[1,\ell]} a'_{k,\,j} g_k$ mit $a_{j,i}\,,\; a'_{k,\,j} \,\in\, A$. Dann wird

$$\sum_{k\in[1,\ell]} \partial_{k,i}\, g_k \;=\; g_i \;=\; \sum_{j\in[1,\ell]} \sum_{k\in[1,\ell]} a_{j,i}\, a'_{k,\,j}\, g_k \;,$$

also $\partial_{k,i} \;=\; \sum_{j\in[1,\ell]} a'_{k,\,j} a_{j,i}$ für $i,\, k \,\in\, [1,\ell]$. Mit $T := (a_{j,i})_{j,i}\,,\; T' := (a'_{k,\,j})_{k,\,j} \,\in\, A^{\ell\times\ell}$ ist also $T'T = \mathrm{E}_\ell$. Es folgt $\det(T')\det(T) = 1$ und somit $\det(T) \in \mathrm{U}(A)$.

Nun ist

$$\tau_k(g_i) \;=\; \tau_k\Big(\sum_{j\in[1,\ell]} a_{j,i}\, h_j\Big) \;=\; \sum_{j\in[1,\ell]} a_{j,i}\, \tau_k(h_j)$$

für $k,\, i \,\in\, [1,\ell]$ und also

$$\mathrm{Vand}_{L|K,\,\underline{g}} \;=\; (\tau_k(g_i))_{i,k} \;=\; (a_{j,i})_{i,\,j} \cdot (\tau_k(h_j))_{j,k} \;=\; T^{\mathrm{t}}\, \mathrm{Vand}_{L|K,\,\underline{h}}\;,$$

woraus

$$\det(\mathrm{Vand}_{L|K,\underline{g}}) \;=\; \det(T)\det(\mathrm{Vand}_{L|K,\underline{h}})$$

und also

$$\Delta_{L|K,\underline{g}} \;=\; \det(T)^2\Delta_{L|K,\underline{h}}$$

folgt; cf. Lemma 24. □

Definition 37 Ist $A = \mathbf{Z}$, $K = \mathbf{Q}$ und $\underline{g} := (\, g_i \,:\, i \in [1,\ell]\,)$ eine $\mathbf{Z}$-lineare Basis von $B = \mathcal{O}_L$, so heißt die Diskriminante

$$\Delta_L := \Delta_{L|\mathbf{Q},\underline{g}} \;\in\; \mathbf{Z}\,,$$

von $\mathcal{O}_L|\mathbf{Z}$ auch kurz die Diskriminante von L.

Sie ist von der Wahl von $\underline{g}$ unabhängig, da $e^2 = 1$ für $e \in \mathrm{U}(\mathbf{Z}) = \{-1,+1\}$; cf. Lemma 36.

Beispiel 38

(1) Es ist $\Delta_{\mathbf{Q}(\mathrm{i})} = -4$, da $(1,\mathrm{i})$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\mathrm{i})} = \mathbf{Z}[\mathrm{i}]$ ist; cf. Beispiele 23 und 26.

(2) Wir wollen $\Delta_{\mathbf{Q}(\sqrt{5})}$ berechnen. Schreibe $\alpha := \frac{1+\sqrt{5}}{2}$. Es ist $\underline{y} := (1,\alpha)$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Das Element von Ordnung 2 in $\mathrm{Gal}(\mathbf{Q}(\sqrt{5})|\mathbf{Q})$ schickt $\sqrt{5}$ auf $-\sqrt{5}$ und somit α auf $1-\alpha$. Es ist

$$\mathrm{Vand}_{\mathbf{Q}(\sqrt{5})|\mathbf{Q},\underline{y}} \;=\; \left(\begin{smallmatrix} 1 & 1 \\ \alpha & 1-\alpha \end{smallmatrix}\right)$$

und somit

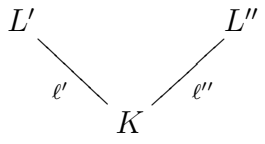
$$\Delta_{\mathbf{Q}(\sqrt{5})} \;=\; \Delta_{\mathbf{Q}(\sqrt{5})|\mathbf{Q},(1,\alpha)} \;=\; \det(\mathrm{Vand}_{\mathbf{Q}(\sqrt{5})|\mathbf{Q},\underline{y}})^2 \;=\; (1-2\alpha)^2 \;=\; (-\sqrt{5})^2 \;=\; 5\,.$$

1.4 Komposita

Sei K ein perfekter Körper. Seien $L'|K$ und $L''|K$ endliche Körpererweiterungen.

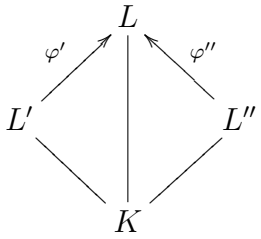
Sei $\ell' := [L' : K]$. Sei $\underline{y'} = (\, y'_i \,:\, i \in [1,\ell']\,)$ eine K-lineare Basis von L'.

Sei $\ell'' := [L'' : K]$. Sei $\underline{y''} = (\, y''_j \,:\, j \in [1,\ell'']\,)$ eine K-lineare Basis von L''.



1.4.1 Komposita von Körpererweiterungen

Definition 39 Eine Körpererweiterung $L|K$, zusammen mit Körpermorphismen $\varphi' : L' \longrightarrow L$ mit $\varphi'|_K^K = \mathrm{id}_K$ und $\varphi'' : L'' \longrightarrow L$ mit $\varphi''|_K^K = \mathrm{id}_K$, heißt *Kompositum* von $L'|K$ und $L''|K$, falls der einzige Teilkörper von L, der $\varphi'(L')$ und $\varphi''(L'')$ enthält, gleich L ist.



Ist also diesenfalls F ein Teilkörper von L mit $\varphi'(L') \subseteq F$ und $\varphi''(L'') \subseteq F$, dann ist bereits $F = L$. Man sagt auch, $\varphi'(L')$ und $\varphi''(L'')$ *erzeugen* den Körper L.

Lemma 40 *Es gibt ein Kompositum $L|K$ von $L'|K$ und $L''|K$ via gewisser Körpermorphismen $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$.*

Beweis. Sei E' Zerfällungskörper von $L'|K$. Sei E'' Zerfällungskörper von $L''|K$. Cf. Lemma 11.(1, 2).

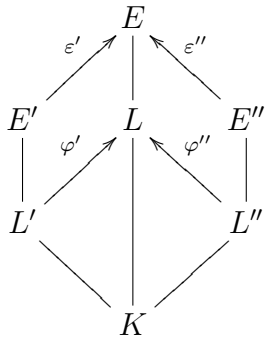
Es sind $E'|K$ und $E''|K$ galoisch. Also ist $E'|K$ Zerfällungskörper eines normierten Polynoms $f_1(X) \in K[X]$; und es ist $E''|K$ Zerfällungskörper eines normierten Polynoms $f_2(X) \in K[X]$; cf. **[5,** §3.5.1.4]. Sei E Zerfällungskörper von $f_1(X)f_2(X) \in K[X]$; cf. **[5,** §2.5.2].

Sei $\tilde{E}'$ das Erzeugnis der Nullstellen von $f_1(X)$ in E. Dann ist auch $\tilde{E}'$ Zerfällungskörper von $f_1(X) \in K[X]$. Also können wir einen Isomorphismus $E' \xrightarrow{\sim} \tilde{E}'$ wählen, der auf K identisch einschränkt; cf. **[5,** §3.5.1.4]. Sei $\varepsilon' : E' \longrightarrow E$ sein Kompositum mit der Einbettung $\tilde{E}' \hookrightarrow E$.

Sei $\tilde{E}''$ das Erzeugnis der Nullstellen von $f_2(X)$ in E. Dann ist auch $\tilde{E}''$ Zerfällungskörper von $f_2(X) \in K[X]$. Also können wir einen Isomorphismus $E'' \xrightarrow{\sim} \tilde{E}''$ wählen, der auf K identisch einschränkt; cf. loc. cit. Sei $\varepsilon'' : E'' \longrightarrow E$ sein Kompositum mit der Einbettung $\tilde{E}'' \hookrightarrow E$.

Sei L der kleinste Teilkörper von E, der $\varepsilon'(L')$ und $\varepsilon''(L'')$ enthält.

Sei $\varphi' := \varepsilon'|_{L'}^{L}$. Sei $\varphi'' := \varepsilon''|_{L''}^{L}$. Dann ist L der kleinste Teilkörper von L, der $\varphi'(L') = \varepsilon'(L')$ und $\varphi''(L'') = \varepsilon''(L'')$ enthält.



□

Beispiel 41

(1) Sind in der Situation von Definition 39 die Abbildungen φ' resp. φ'' Einbettungen von Teilkörpern L' resp. L'' in L, dann ist L ein Kompositum von $L'|K$ und $L''|K$, wenn L der kleinste Teilkörper von L ist, der L' und L'' enthält.

(2) Es ist $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)|\mathbf{Q}$ Kompositum von $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ und $\mathbf{Q}(\zeta_3)|\mathbf{Q}$, via der Einbettungen.

(3) Es ist $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)|\mathbf{Q}$ Kompositum von $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ und $\mathbf{Q}(\zeta_3\sqrt[3]{2})|\mathbf{Q}$, via der Einbettungen.

(4) Es ist $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ Kompositum von $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ und $\mathbf{Q}(\zeta_3\sqrt[3]{2})|\mathbf{Q}$, via der Identität und via $\mathbf{Q}(\zeta_3\sqrt[3]{2}) \xrightarrow{\sim} \mathbf{Q}(\sqrt[3]{2})$, $\zeta_3\sqrt[3]{2} \longmapsto \sqrt[3]{2}$; cf. Lösung zu Aufgabe 7.

Insbesondere zeigen (3) und (4), daß ein Kompositum zweier Körpererweiterungen nicht bis auf Isomorphie eindeutig bestimmt ist. Cf. aber Lemma 47.(1) unten.

Bemerkung 42 *Sei $L|K$ ein Kompositum von $L'|K$ und $L''|K$ via $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$.*

Dann ist

$$L \;=\; {}_K\langle\, \varphi'(y'_i) \cdot \varphi''(y''_j) \;:\; i \in [1, \ell'],\, j \in [1, \ell'']\,\rangle$$

Insbesondere ist $[L : K] \leqslant [L' : K] \cdot [L'' : K]$.

Insbesondere ist $L|K$ eine endliche Körpererweiterung.

Beweis. Wir haben

$$L \;\overset{!}{\subseteq}\; {}_K\langle\, \varphi'(y'_i) \cdot \varphi''(y''_j) \;:\; i \in [1, \ell'],\, j \in [1, \ell'']\,\rangle$$

zu zeigen.

Schreibe $L'' = K(z'')$ für ein geeignetes $z'' \in L''$; cf. [**5,** Aufgabe 54].

Schreibe $w'' := \varphi''(z'')$. Dann ist $\varphi''(L'') = K(w'')$.

Ein Teilkörper von L enthält also genau dann $\varphi''(L'')$, wenn er K und w'' enthält. Somit wird

$$L \;=\; \varphi'(L')(w'') \;.$$

Da z'' algebraisch ist über K, ist auch w'' algebraisch über K, a fortiori also algebraisch über $\varphi'(L')$.

Jedes Element von L ist mithin ein polynomialer Ausdruck in w'' mit Koeffizienten in $\varphi'(L')$.

Jeder dazu benötigte Koeffizient liegt in $\varphi'(L') = {}_K\langle\, \varphi'(y'_i) \,:\, i \in [1,\ell']\,\rangle$.

Jede dazu benötigte Potenz von w'' liegt in

$$K(w'') \;=\; \varphi''(K(z'')) \;=\; \varphi''({}_K\langle\, y''_j \,:\, j \in [1,\ell'']\,\rangle) \;=\; {}_K\langle\, \varphi''(y''_j) \,:\, j \in [1,\ell'']\,\rangle \;.$$

Besagte Linearkombination liegt also in ${}_K\langle\, \varphi'(y'_i)\cdot\varphi''(y''_j) \,:\, i \in [1,\ell'],\, j \in [1,\ell'']\,\rangle$. ▫

1.4.2 Komposita linear disjunkter Körpererweiterungen

Definition 43 Die Körpererweiterungen $L'|K$ und $L''|K$ heißen *linear disjunkt,* wenn für alle $z'' \in L''$ das Minimalpolynom $\mu_{z'',K}(X) \in K[X]$ auch in $L'[X]$ noch irreduzibel ist.

Lemma 44 Sei $L|K$ ein Kompositum von $L'|K$ und $L''|K$, via $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$.

Es sind $L'|K$ und $L''|K$ linear disjunkt genau dann, wenn $[L:K] = [L':K]\cdot[L'':K]$ ist.

> Insbesondere sind $L'|K$ und $L''|K$ genau dann linear disjunkt, wenn $L''|K$ und $L'|K$ linear disjunkt sind. Die nichtsymmetrische Definition ist also nur etwas unschön.

Beweis. Sei $L' = K(z')$ mit einem geeigneten $z' \in L'$; sei $L'' = K(z'')$ mit einem geeigneten $z'' \in L''$; cf. [**5,** Aufgabe 54]. Schreibe $w' := \varphi'(z')$ und $w'' := \varphi''(z'')$. Dann ist $\varphi'(L') = K(w')$, es ist $\varphi''(L'') = K(w'')$ und es ist $L = K(w',w'')$.

Ad $\Rightarrow$. Es ist $\mu_{z'',K}(X) = \mu_{w'',K}(X)$ irreduzibel auch noch in $\varphi'(L')[X] = K(w')[X]$ und also gleich $\mu_{w'',K(w')}(X)$. Folglich ist

$$[K(w',w'') : K(w')] \;=\; \deg(\mu_{w'',K(w')}) \;=\; \deg(\mu_{z'',K}) \;=\; [K(z'') : K] \;=\; [L'' : K]$$

und somit

$$\begin{aligned}[K(w',w'') : K] \;&=\; [K(w',w'') : K(w')]\cdot[K(w') : K] \\ &=\; [K(w',w'') : K(w')]\cdot[K(z') : K] \;=\; [L'' : K]\cdot[L' : K]\;.\end{aligned}$$

Ad $\Leftarrow$. Sei $[L:K] = [L':K]\cdot[L'':K]$. *Annahme,* es sind $L'|K$ und $L''|K$ nicht linear disjunkt. Sei $u'' \in L''$ mit $\mu_{u'',K}(X)$ reduzibel in $L'[X]$. Schreibe $v'' := \varphi''(u'')$. Dann ist

auch $\mu_{v'',K}(X) = \mu_{u'',K}(X)$ reduzibel in $L'[X]$, und somit auch in $K(w')[X]$. Somit muß $\mu_{v'',K(w')}(X)$ ein echter Teiler von $\mu_{v'',K}(X)$ sein. Also ist

$$[K(w',v'') : K(w')] \;=\; \deg(\mu_{v'',K(w')}) \;<\; \deg(\mu_{v'',K}) \;=\; [K(v'') : K] \;=\; [K(u'') : K]\,.$$

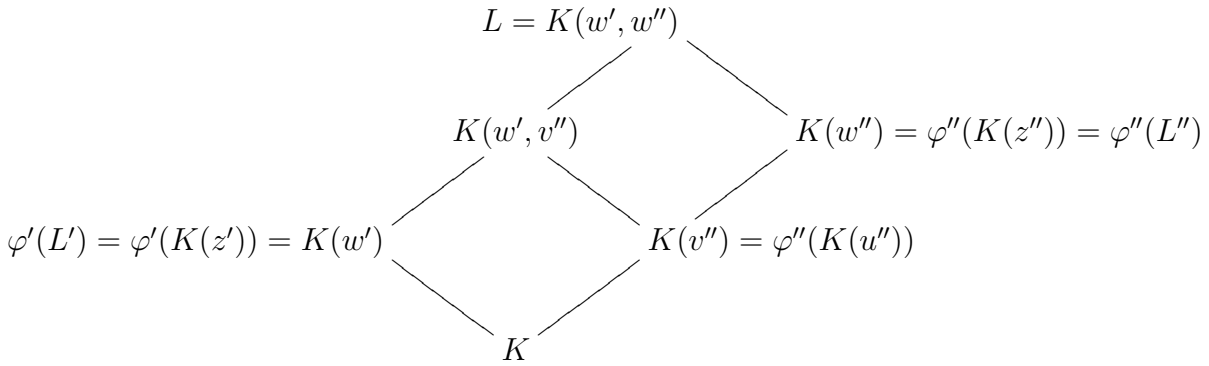
Ferner ist $\mu_{w'',K(w',v'')}(X)$ ein Teiler von $\mu_{w'',K(v'')}(X)$ und somit

$$\begin{aligned}[K(w',w'') : K(w',v'')] \;&=\; \deg(\mu_{w'',K(w',v'')}) \;\leqslant\; \deg(\mu_{w'',K(v'')}) \\ &=\; [K(w'') : K(v'')] \;=\; [K(z'') : K(u'')] \;=\; [L'' : K(u'')]\,.\end{aligned}$$

Zusammen wird also

$$\begin{aligned}[L : K] \;=\; [K(w',w'') : K] \;&=\; [K(w',w'') : K(w',v'')] \cdot [K(w',v'') : K(w')] \cdot [K(w') : K] \\ &<\; [L'' : K(u'')] \cdot [K(u'') : K] \cdot [K(z') : K] \;=\; [L'' : K] \cdot [L' : K]\,,\end{aligned}$$

und wir haben einen *Widerspruch.*



□

Beispiel 45

(1) Es sind $\mathbf{Q}(\sqrt[3]{2})$ und $\mathbf{Q}(\zeta_3)$ linear disjunkt, da wir als Kompositum $L = \mathbf{Q}(\sqrt[3]{2},\zeta_3)|\mathbf{Q}$ nehmen können und da $[\mathbf{Q}(\sqrt[3]{2},\zeta_3) : \mathbf{Q}] = 6 = 3 \cdot 2 = [\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] \cdot [\mathbf{Q}(\zeta_3) : \mathbf{Q}]$ ist; cf. Aufgabe 7.

(2) Es sind $L'|K$ und $L'|K$ linear disjunkt genau dann, wenn $L' = K$ ist. Denn wir können als Kompositum ebenfalls $L = L'|K$ wählen.

(3) Es sind $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ und $\mathbf{Q}(\zeta_3\sqrt[3]{2})|\mathbf{Q}$ nicht linear disjunkt. Denn es ist $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ und $[\mathbf{Q}(\zeta_3\sqrt[3]{2}) : \mathbf{Q}] = 3$, aber das für das Kompositum aus Beispiel 41.(3) ist $[\mathbf{Q}(\sqrt[3]{2},\zeta_3) : \mathbf{Q}] = 6 \neq 3 \cdot 3$; cf. Aufgabe 7.

Alternativ hätte man auch das Kompositum aus Beispiel 41.(4) heranziehen können, um damit festzustellen, daß auch $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3 \neq 3 \cdot 3$ ist.

Abermals alternativ hätte man auch feststellen können, daß $\mu_{\zeta_3\sqrt[3]{2},\mathbf{Q}}(X) = X^3 - 2$ in $\mathbf{Q}(\sqrt[3]{2})$ die Nullstelle $\sqrt[3]{2}$ hat und folglich reduzibel ist, um zu zeigen, daß $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ und $\mathbf{Q}(\zeta_3\sqrt[3]{2})|\mathbf{Q}$ nicht linear disjunkt sind.

Beachte, daß nichtsdestotrotz $\mathbf{Q}(\sqrt[3]{2}) \cap \mathbf{Q}(\zeta_3\sqrt[3]{2}) = \mathbf{Q}$ ist, da kein weiterer Zwischenkörper in den beiden Teilnehmern des Schnitts enthalten sind, i.e. da $(1,3)$ und $(2,3)$ die Gruppe S_3 erzeugen; cf. Aufgabe 7.

Korollar 46 *Sei $L|K$ ein Kompositum von $L'|K$ und $L''|K$ via $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$.*

Es sind $L'|K$ und $L''|K$ genau dann linear disjunkt, wenn

$$(\varphi'(y'_i) \cdot \varphi''(y''_j) \,:\, i \in [1, \ell'],\, j \in [1, \ell''])$$

eine K-lineare Basis von L ist.

Beweis. Wegen Bemerkung 42 ist genau dann $[L : K] = [L' : K] \cdot [L'' : K]$, wenn das K-lineare Erzeugendensystem $(\varphi'(y'_i) \cdot \varphi''(y''_i) \,:\, i \in [1, \ell'],\, j \in [1, \ell''])$ von L auch K-linear unabhängig ist. ▫

Lemma 47 *Seien $L'|K$ und $L''|K$ linear disjunkt.*

Sei $L|K$, via $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$, ein Kompositum von $L'|K$ und $L''|K$.

(1) *Ist $\tilde{L}|K$, via $\tilde{\varphi}' : L' \longrightarrow \tilde{L}$ und $\tilde{\varphi}'' : L'' \longrightarrow \tilde{L}$, ein weiteres Kompositum von $L'|K$ und $L''|K$, dann gibt es einen eindeutigen Körpermorphismus $\alpha : L \longrightarrow \tilde{L}$ mit $\alpha \circ \varphi' = \tilde{\varphi}'$ und $\alpha \circ \varphi'' = \tilde{\varphi}''$. Dieser ist ein Isomorphismus $\alpha : L \xrightarrow{\sim} \tilde{L}$.*

(2) *Ist $M|K$ eine endliche Körpererweiterung und sind Körpermorphismen $L' \xrightarrow{\psi'} M$ und $L'' \xrightarrow{\psi''} M$ mit $\psi'|_K^K = \psi''|_K^K = \mathrm{id}_K$ gegeben, dann gibt es einen eindeutigen Körpermorphismus $\beta : L \longrightarrow M$ mit $\beta \circ \varphi' = \psi'$ und $\beta \circ \varphi'' = \psi''$.*

Beweis. Cf. Aufgabe 20. ▫

1.4.3 Komposita linear disjunkter Erweiterungen und ganze Elemente

Seien $L'|K$ und $L''|K$ linear disjunkt.

Sei $A \subseteq K$ ein ganzabgeschlossener Teilring mit $K = \mathrm{Quot}(A)$.

Sei $B' := \Gamma_{L'}(A)$. Sei $B'' := \Gamma_{L''}(A)$.

Sei $\underline{g'} = (g'_i \,:\, i \in [1, \ell'])$ eine A-lineare Basis von B'.

Sei $\underline{g''} = (g''_i \,:\, i \in [1, \ell''])$ eine A-lineare Basis von B''.

Die Existenz solcher Basen ist garantiert, sofern A ein Hauptidealbereich ist; cf. Lemma 33.

Sei L eine gemeinsame Körpererweiterung von L' und L'', welche ein Kompositum von $L'|K$ und $L''|K$ ist, mit den Inklusionen $L' \hookrightarrow L$ und $L'' \hookrightarrow L$; cf. Definition 39.

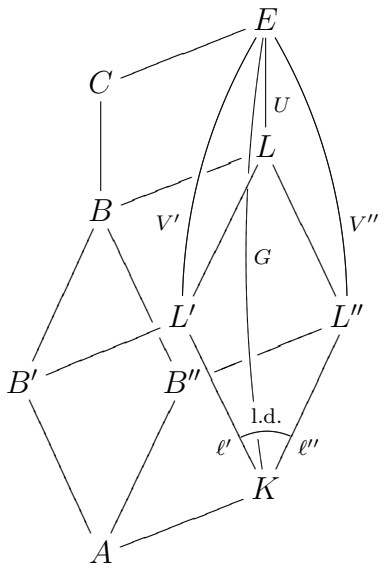
Um ausgehend von $L'|K$ und $L''|K$ eine solche Situation zu erreichen, kann man e.g. via Lemma 40 ein Kompositum dieser Erweiterungen konstruieren und dann die Körper L' und L'' isomorph duch Teilkörper dieses Kompositums ersetzen.

Sei $B := \Gamma_L(A)$. Es ist $B' = B \cap L'$ und $B'' = B \cap L''$.

Sei E ein Zerfällungskörper von $L|K$; cf. Lemma 11.(1, 2). Sei $C := \Gamma_E(A)$.

Sei $G := \mathrm{Gal}(E|K)$, sei $U := \mathrm{Gal}(E|L)$, sei $V' := \mathrm{Gal}(E|L')$, sei $V'' := \mathrm{Gal}(E|L'')$.

Schreibe $G = \bigsqcup_{i\in[1,\ell']} \tau'_i V'$ mit $\tau'_i \in G$ für $i \in [1, \ell']$. Schreibe $G = \bigsqcup_{j\in[1,\ell'']} \tau''_j V''$ mit $\tau''_j \in G$ für $j \in [1, \ell'']$.



Satz 48 (Diskriminante des Kompositums)

Wir erinnern daran, daß A ganzabgeschlossen ist, $K = \mathrm{Quot}(A)$ perfekt ist und die endlichen Körpererweiterungen $L'|K$ und $L''|K$ linear disjunkt sind. Bekanntlich nennen wir $\ell' = [L' : K]$ und $\ell'' = [L'' : K]$. Wir erinnern ferner an die A-lineare Basis $\underline{g'}$ von $B' = \Gamma_{L'}(A)$ und an die A-lineare Basis $\underline{g''}$ von $B'' = \Gamma_{L''}(A)$.

Seien die Diskriminanten von $L'|K$ und $L''|K$ in folgendem Sinne teilerfremd. Es gebe s', $s'' \in A$ mit

$$s'\Delta_{L'|K,\underline{g'}} + s''\Delta_{L''|K,\underline{g''}} \;=\; 1\ .$$

(1) *Es ist*

$$\underline{g} \;:=\; (\, g'_i\, g''_j \;:\; i \in [1,\ell'],\, j \in [1,\ell'']\,)$$

eine A-lineare Basis von B.

(2) *Es ist*

$$\Delta_{L|K,\,\underline{g}} \;=\; (\Delta_{L'|K,\,\underline{g'}})^{\ell''} \cdot (\Delta_{L''|K,\,\underline{g''}})^{\ell'} \;.$$

Die Bedingung an die Teilerfremdheit der Diskriminanten kann hierbei nicht entfallen; cf. Lösung zu Aufgabe 62.

Beweis.

Ad (1). Da $\underline{g'}$ eine K-lineare Basis von L' ist, da $\underline{g''}$ eine K-lineare Basis von L'' ist und da $L'|K$ und $L''|K$ linear disjunkt sind, ist $\underline{g}$ eine K-lineare Basis von L; cf. Korollar 46.

Wir haben $B \overset{!}{\subseteq} {}_A\langle \underline{g} \rangle$ zu zeigen.

Sei ein Element $b \in B$ gegeben. Schreibe $b =: \sum_{i\in[1,\ell']} \sum_{j\in[1,\ell'']} x_{i,\,j} g'_i g''_j$ mit $x_{i,\,j} \in K$ stets.

Wir haben zu zeigen, daß $x_{i,\,j} \overset{!}{\in} A$ liegt für $i \in [1,\ell']$ und $j \in [1,\ell'']$.

Schreibe $d' := \Delta_{L'|K,\,\underline{g'}}$ und $d'' := \Delta_{L''|K,\,\underline{g''}}$. Da es s', $s'' \in A$ gibt mit $s'd' + s''d'' = 1$, genügt es zu zeigen, daß $d'x_{i,\,j} \overset{!}{\in} A$ und $d''x_{i,\,j} \overset{!}{\in} A$ liegen für $i \in [1,\ell']$ und $j \in [1,\ell'']$. Wegen der Symmetrie der Situation genügt es zu zeigen, daß stets $d''x_{i,\,j} \overset{!}{\in} A$ liegt.

Schreibe $y'_j := \sum_{i\in[1,\ell']} x_{i,\,j}\, g'_i$ für $j \in [1,\ell'']$. Wir müssen $d''y'_j = \sum_{i\in[1,\ell']} (d''x_{i,\,j}) g'_i \overset{!}{\in} B'$ zeigen für $j \in [1,\ell'']$, da $\underline{g'}$ eine A-lineare Basis von B' ist. Da $B' = L' \cap C$ ist, genügt es, $d''y'_j \overset{!}{\in} C$ zu zeigen für $j \in [1,\ell'']$.

Sei $\sigma_k : L \longrightarrow E$ der Körpermorphismus mit $\sigma_k|_{L'} = \mathrm{id}_E\,|_{L'}$ und $\sigma_k|_{L''} = \tau''_k|_{L''}$ für $k \in [1,\ell'']$; cf. Lemma 47.(2).

Wähle einen Körpermorphismus $\rho_k : E \longrightarrow E$ mit $\rho_k|_L = \sigma_k$ für $k \in [1,\ell'']$; cf. Lemma 11.(3).

Da ρ_k als Körpermorphismus injektiv ist, da ρ_k eine K-lineare Abbildung ist und da $[E:K]$ endlich ist, ist ρ_k stets ein Isomorphismus, i.e. $\rho_k \in G$ für $k \in [1,\ell'']$.

Für $k \in [1,\ell'']$ wird

$$C \overset{\text{L. 20.(1)}}{\ni} \rho_k(b) \;=\; \sum_{i\in[1,\ell']} \sum_{j\in[1,\ell'']} \rho_k(x_{i,\,j})\rho_k(g'_i)\rho_k(g''_j) \;=\; \sum_{i\in[1,\ell']} \sum_{j\in[1,\ell'']} x_{i,\,j}\, g'_i\, \tau_k(g''_j) \;=\; \sum_{j\in[1,\ell'']} \tau_k(g''_j) y'_j \;.$$

Sei $y' = (y'_j)_j \in {L'}^{\ell''\times 1}$. Wir haben $d''y' \overset{!}{\in} C^{\ell\times 1}$ zu zeigen.

Mit den getroffenen Wahlen ist $\mathrm{Vand}_{L''|K,\,\underline{g''}} = (\tau''_k(g''_j))_{j,k} \in C^{\ell''\times\ell''}$. Ihre Determinante ist $\det(\mathrm{Vand}_{L''|K,\,\underline{g''}})^2 = d''$ cf. Lemma 24.

In Matrix und Vektor zusammengefaßt wird

$$(\mathrm{Vand}_{L''|K,\,\underline{g''}})^{\mathrm{t}}\, y' \;\in\; C^{\ell''\times 1} \;.$$

Dank Cramerscher Regel gibt es eine Matrix $S \in C^{\ell'' \times \ell''}$ mit $S \cdot (\mathrm{Vand}_{L''|K,\underline{g''}})^{\mathrm{t}} = \det(\mathrm{Vand}_{L''|K,\underline{g''}})\mathrm{E}_{\ell''}$; cf. Aufgabe 1.(2). Mit $T := \det(\mathrm{Vand}_{L''|K,\underline{g''}})S \in C^{\ell'' \times \ell''}$ wird $T \cdot (\mathrm{Vand}_{L''|K,\underline{g''}})^{\mathrm{t}} = d''\mathrm{E}_{\ell''}$. Somit ist auch

$$d''y' \;=\; T \cdot (\mathrm{Vand}_{L''|K,\underline{g''}})^{\mathrm{t}}\, y' \;\in\; C^{\ell'' \times 1} \;.$$

Ad (2). Wir *behaupten* $U \stackrel{!}{=} V' \cap V''$. Zu zeigen ist nur $\stackrel{!}{\supseteq}$. Sei $\sigma \in G$ mit $\sigma(y') = y'$ für $y' \in L'$ und $\sigma(y'') = y''$ für $y'' \in L''$ gegeben. Schreibe $\mathrm{Fix}_\sigma(L) := \{\, y \in L \,:\, \sigma(y) = y \,\}$. Es ist $\mathrm{Fix}_\sigma(L)$ ein Teilkörper von L. Es sind L' und L'' in $\mathrm{Fix}_\sigma(L)$ enthalten. Da L Kompositum von L' und L'' ist, folgt $\mathrm{Fix}_\sigma(L) = L$, i.e. $\sigma \in U$. Dies zeigt die *Behauptung.*

Wir *behaupten* die Existenz der bijektiven Abbildung

$$\begin{array}{rcccc} G/U & \longrightarrow & (G/V') & \times & (G/V'') \\ \sigma U & \longmapsto & (\sigma V' & , & \sigma V'') \,. \end{array}$$

Diese ist wohldefiniert und injektiv, da für $\sigma, \tau \in G$ genau dann $\sigma U = \tau U$ ist, wenn $\sigma^{-1}\tau \in U = V' \cap V''$ liegt, i.e. wenn $\sigma^{-1}\tau \in V'$ und $\sigma^{-1}\tau \in V''$ liegen, i.e. wenn $\sigma V' = \tau V'$ und $\sigma V'' = \tau V''$ ist. Ferner ist $|G/U| = [L : K] \stackrel{\text{L. 44}}{=} [L' : K] \cdot [L'' : K] = |G/V'| \cdot |G/V''| = |(G/V') \times (G/V'')|$. Dies zeigt die *Behauptung.*

> Alternativ erkennt man die Surjektivität dieser Abbildung auch folgendermaßen. Sei $(\sigma'V', \sigma''V'') \in (G/V') \times (G/V'')$ gegeben. Sei $\sigma : L \to E$ der Körpermorphismus mit $\sigma|_{L'} = \sigma'|_{L'}$ und $\sigma|_{L''} = \sigma''|_{L''}$; cf. Lemma 47.(2). Sei $\rho : E \to E$ ein Körpermorphismus mit $\rho|_L = \tau$; cf. Lemma 11.(3). Es ist $\rho \in G$ mit $\rho|_{L'} = \sigma'|_{L'}$ und $\rho|_{L''} = \sigma''|_{L''}$, i.e. $\rho V' = \sigma' V'$ und $\rho V'' = \sigma V''$.

Für $(i, j) \in [1, \ell'] \times [1, \ell'']$ sei $\tau_{(i,j)} \in G$ mit $\tau_{(i,j)}V' = \tau'_i V'$ und $\tau_{(i,j)}V'' = \tau''_j V''$ gewählt. Dank vorstehender Behauptung ist auch $G = \bigsqcup_{(i,j)\in[1,\ell']\times[1,\ell'']} \tau_{(i,j)}U$.

Schreibe $\ell := [L : K] = \ell' \cdot \ell''$. Wir wählen eine Bijektiion

$$\begin{array}{rcl} [1, \ell] & \stackrel{\alpha}{\tilde{\longrightarrow}} & [1, \ell'] \times [1, \ell''] \\ k & \longmapsto & \alpha(k) \;=:\; (\alpha'(k), \alpha''(k)) \end{array}$$

Mit ihr wird $G = \bigsqcup_{k\in[1,\ell]} \tau_{\alpha(k)}U$. Wir präzisieren noch die Anordnung der Elemente in $\underline{g}$ zu

$$\underline{g} \;=\; (\, g'_{\alpha'(k)}\, g''_{\alpha''(k)} \;:\; k \in [1, \ell]\,) \;.$$

> Die Diskriminante ist von der Wahl dieser Anordnung unabhängig, da eine andere Wahl nur ein Wechsel des Vorzeichens in der Determinante der Vandermondematrix verursachen kann.

So wird in $E^{\ell\times\ell}$

$$\begin{aligned}
\mathrm{Vand}_{L|K,\underline{g}} &= (\tau_{\alpha(n)}(g'_{\alpha'(k)}\cdot g''_{\alpha''(k)}))_{k,n}\\
&= (\tau_{\alpha(n)}(g'_{\alpha'(k)})\cdot\tau_{\alpha(n)}(g''_{\alpha''(k)}))_{k,n}\\
&= (\tau'_{\alpha'(n)}(g'_{\alpha'(k)})\cdot\tau''_{\alpha''(n)}(g''_{\alpha''(k)}))_{k,n}\\
&= (\textstyle\sum_{m\in[1,\ell]}\tau'_{\alpha'(n)}(g'_{\alpha'(m)})\cdot\partial_{\alpha''(n),\,\alpha''(m)}\cdot\partial_{\alpha'(m),\,\alpha'(k)}\cdot\tau''_{\alpha''(m)}(g''_{\alpha''(k)}))_{k,n}\\
&= ((\textstyle\sum_{m\in[1,\ell]}\tau'_{\alpha'(n)}(g'_{\alpha'(m)})\cdot\partial_{\alpha''(n),\,\alpha''(m)}\cdot\partial_{\alpha'(m),\,\alpha'(k)}\cdot\tau''_{\alpha''(m)}(g''_{\alpha''(k)}))_{n,k})^{\mathrm{t}}\\
&= ((\tau'_{\alpha'(n)}(g'_{\alpha'(m)})\partial_{\alpha''(n),\,\alpha''(m)})_{n,m}\cdot(\partial_{\alpha'(m),\,\alpha'(k)}\tau''_{\alpha''(m)}(g''_{\alpha''(k)}))_{m,k})^{\mathrm{t}}\ .
\end{aligned}$$

Mit Aufgabe 21 wird über eine Blockdiagonalmatrixüberlegung

$$\begin{aligned}
\det((\tau'_{\alpha'(n)}(g'_{\alpha'(m)})\partial_{\alpha''(n),\,\alpha''(m)})_{n,m}) &= \det((\tau'_j(g'_i))_{i,\,j})^{\ell''} = \det(\mathrm{Vand}_{L'|K,\underline{g'}})^{\ell''}\\
\det((\partial_{\alpha'(m),\,\alpha'(k)}\tau''_{\alpha''(m)}(g''_{\alpha''(k)}))_{m,k}) &= \det((\tau''_j(g''_i))_{i,\,j})^{\ell'} = \det(\mathrm{Vand}_{L''|K,\underline{g''}})^{\ell'}\ .
\end{aligned}$$

Mit Lemma 24 wird

$$\Delta_{L|K,\underline{g}} = \det(\mathrm{Vand}_{L|K,\underline{g}})^2 = \det(\mathrm{Vand}_{L'|K,\underline{g'}})^{2\ell''}\cdot\det(\mathrm{Vand}_{L''|K,\underline{g''}})^{2\ell'} = (\Delta_{L'|K,\underline{g'}})^{\ell''}\cdot(\Delta_{L''|K,\underline{g''}})^{\ell'}\ .$$

□

Kapitel 2

Ideale

2.1 Dedekindbereiche

Lemma 49 *Sei R ein kommutativer Ring. Die Aussagen* (1) *und* (2) *sind äquivalent.*

(1) *Jedes Ideal in R ist endlich erzeugt.*

(2) *Jede nichtleere Teilmenge von* Ideale(R) *hat ein maximales Element.*

Beweis. Cf. Aufgabe 24.(1). □

Definition 50 Ein kommutativer Ring, der eine der äquivalenten Bedingungen von Lemma 49 erfüllt, heißt *noethersch.*

Bemerkung 51 Sei R ein kommutativer Ring.

(1) Ist R ein Hauptidealbereich, dann ist R noethersch. Cf. auch Aufgabe 2.(1).

(2) Ist R noethersch, dann ist auch $R[X]$ noethersch; cf. Aufgabe 24.(2).

(3) Ist R noethersch und $\mathfrak{a} \subseteq R$ ein Ideal, dann ist auch $R/\mathfrak{a}$ noethersch; cf. Aufgabe 24.(3).

(4) Ist R noethersch und $\mathfrak{a} \subset R$ ein Ideal, dann gibt es ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m} \subset R$.

Denn $\{\, \mathfrak{b} \in \text{Ideale}(R) : \mathfrak{a} \subseteq \mathfrak{b} \subset R \,\}$ enthält $\mathfrak{a}$, ist daher nichtleer und enthält somit wegen R noethersch ein maximales Element $\mathfrak{m}$. Dieses ist dann auch maximal in Ideale(R)$\setminus\{(1)\}$, denn für $\mathfrak{m}' \in \text{Ideale}(R)\setminus\{(1)\}$ mit $\mathfrak{m} \subseteq \mathfrak{m}'$ folgt $\mathfrak{a} \subseteq \mathfrak{m} \subseteq \mathfrak{m}' \subset R$, nach Wahl von $\mathfrak{m}$ also $\mathfrak{m} = \mathfrak{m}'$. ([2])

[2]Das Lemma von Zorn muß für diese Aussage im Falle R noethersch also nicht eingesetzt werden. Cf. Behauptung in Lösung zu Aufgabe 13.(1).

Definition 52 Ein ganzabgeschlossener, noetherscher Integritätsbereich, in welchem jedes Primideal ungleich (0) ein maximales Ideal ist, heißt *Dedekindbereich* oder *dedekindsch.*

Cf. Definitionen 7.(2) und 50.

Bemerkung 53 *Jeder Hauptidealbereich ist dedekindsch.*

Beweis. Sei A ein Hauptidealbereich. Es ist A noethersch; cf. Bemerkung 51.(1). Es ist A ganzabgeschlossen; cf. Aufgabe 6.(1).

Weil jedes $\mathfrak{a} \in \mathrm{Ideale}(A) \smallsetminus \{(1)\}$ in einem maximalen Ideal von A enthalten ist gemäß Bemerkung 51.(4) und weil jedes maximale Ideal prim ist, da sein Faktorring ein Körper und also ein Integritätbereich ist, genügt es zu zeigen, daß es keine zwei Elemente von $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$ gibt, deren erstes eine echte Teilmenge des zweiten ist.

Sei ein Primideal in A gegeben. Dieses ist von der Form (p) für ein $p \in A$. Sei ein weiteres Primideal in A gegeben, welches echt in (p) liegt. Dieses ist also von der Form (xp) für ein $x \in A$. Wir haben $(xp) \overset{!}{=} (0)$ zu zeigen. *Annahme,* nicht. Dann sind $x \neq 0$ und $p \neq 0$. Es ist $xp \in (xp)$. Es ist $x \notin (xp)$, da sonst $x = xpa$ für ein $a \in A$ wäre, also $1 = pa$, also $(p) = (1)$, was nicht der Fall ist. Es ist $p \notin (xp)$, da sonst $(p) \subseteq (xp)$ läge und somit $(xp) = (p)$ wäre. Folglich ist (xp) kein Primideal, und wir haben einen *Widerspruch.* ▫

Lemma 54 (Ganzer Abschluß wieder dedekindsch)

Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt.

Sei $L|K$ eine endliche Körpererweiterung. Schreibe $B := \Gamma_L(A)$.

Es ist B ein Dedekindbereich.

Wir haben eine Abbildung $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(B) \longrightarrow \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$, $\mathfrak{q} \longmapsto \mathfrak{q} \cap A$.

Insbesondere ist im Falle $A = \mathbf{Z}$ und $K = \mathbf{Q}$, also im Falle L Zahlkörper, der Zahlring $\mathcal{O}_L = \Gamma_L(\mathbf{Z})$ ein Dedekindbereich.

Beweis. Es ist B als Teilring von L ein Integritätsbereich.

Nach Aufgabe 24.(5) ist auch B noethersch.

Es ist B ganzabgeschlossen; cf. Bemerkung 8.(2).

Sei $\mathfrak{q} \subseteq B$ ein Primideal ungleich (0). Wir haben zu zeigen, daß $\mathfrak{q}$ ein maximales Ideal ist. Schreibe $\mathfrak{p} := A \cap \mathfrak{q}$.

Wir haben einen injektiven Ringmorphismus $\iota : A/\mathfrak{p} \longrightarrow B/\mathfrak{q}$, $a + \mathfrak{p} \longmapsto a + \mathfrak{q}$ in den Integritätsbereich $B/\mathfrak{q}$; beachte, daß für $a \in A$ genau dann $a \in \mathfrak{q}$ liegt, wenn $a \in \mathfrak{p}$ liegt. Da $B/\mathfrak{q}$ ein Integritätsbereich ist, folgt, daß auch $A/\mathfrak{p}$ ein Integritätsbereich ist, i.e. daß $\mathfrak{p}$ ein Primideal in A ist.

Zeigen wir $\mathfrak{p} \overset{!}{\neq} (0)$. Wähle $y \in \mathfrak{q}^{\times}$. Für ein $n \geqslant 1$ ist $\mu_{y,K}(X) =: \sum_{i \in [0,n]} a_i X^i \overset{\text{A. 25.(2)}}{\in} A[X]$. Es ist $a_0 \neq 0$, da sonst X ein Teiler von $\mu_{y,K}(X)$ wäre, was $X = \mu_{y,K}(X)$ und somit $y = 0$

nach sich zöge. Da $y \in \mathfrak{q}$ liegt, liegt auch $a_0 = y \cdot (-\sum_{i\in[1,n]} a_i y^{i-1}) \in \mathfrak{q}$. Insgesamt ist $a_0 \in A^\times \cap \mathfrak{q} = \mathfrak{p}^\times$.

Da A dedekindsch ist, ist $\mathfrak{p} \subseteq A$ ein maximales Ideal; cf. Bemerkung 53. Wir haben zu zeigen, daß $B/\mathfrak{q}$ ein Körper ist. Da B ein endlich erzeugter A-Modul ist, ist $B/\mathfrak{q}$ via ι ein endlichdimensionaler $A/\mathfrak{p}$-Vektorraum; cf. Aufgabe 27.(5). Da $B/\mathfrak{q}$ ein Integritätsbereich ist, ist für $b \in B$ mit $b + \mathfrak{q} \neq 0$ die Abbildung

$$\lambda_{b+\mathfrak{q}} \,:\, B/\mathfrak{q} \longrightarrow B/\mathfrak{q}\,, \quad y+\mathfrak{q} \longmapsto (b+\mathfrak{q})(y+\mathfrak{q})$$

injektiv. Da diese auch $A/\mathfrak{p}$-linear ist, ist sie als injektiver Endomorphismus eines endlichdimensionalen $A/\mathfrak{p}$-Vektorraums sogar bijektiv. Somit ist $B/\mathfrak{q}$ ein Körper. ▫

Beispiel 55 Es ist $\mathbf{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbf{Q}(\sqrt{-5})}$; cf. Aufgabe 3. Also ist $\mathbf{Z}[\sqrt{-5}]$ dedekindsch. Es ist $\mathbf{Z}[\sqrt{-5}]$ aber kein Hauptidealbereich; cf. Aufgabe 6.(4).

2.2 Primidealfaktorzerlegung in Dedekindbereichen

Sei D ein Dedekindbereich. Sei $K := \mathrm{Quot}(D)$.

Definition 56

(1) Ein *gebrochenes Ideal* von D ist eine Teilmenge von K von der Form

$$x\mathfrak{a} := \{\, xa \,:\, a \in \mathfrak{a} \,\}\,,$$

wobei $x \in K^\times$ und $\mathfrak{a} \in \mathrm{Ideale}^\times(D)$ sei. Die Menge der gebrochenen Ideale von D bezeichnen wir mit $\underline{\mathrm{Ideale}}^\times(D)$. Es ist also $\mathrm{Ideale}^\times(D) \subseteq \underline{\mathrm{Ideale}}^\times(D)$.

(2) Für $n \geqslant 1$ und $x_i \in K^\times$ für $i \in [1,n]$ schreiben wir

$$(\, x_1\,,\, \ldots\,,\, x_n\,) \;:=\; \{\, d_1x_1 + \cdots + d_nx_n \,:\, d_i \in D \text{ für } i \in [1,n] \,\}\,.$$

Dies ist ein gebrochenes Ideal, wie man durch Multiplikation mit einem gemeinsamen Nenner der x_i erkennt. Ein gebrochenes Ideal der Form (x) für ein $x \in K^\times$ heißt *gebrochenes Hauptideal* von D.

Liegt $x_i \in D$ für $i \in [1,n]$, so ist das gebrochene Ideal $(\, x_1\,,\, \ldots\,,\, x_n\,)$ das Ideal von D, das bereits diese Bezeichnung trägt.

(3) Seien $\mathfrak{g}$, $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(D)$. Wir setzen

$$\begin{array}{rcl}
\mathfrak{g}^\times & := & \mathfrak{g} \smallsetminus \{0\} \\
\mathfrak{g}\cdot\mathfrak{h} & := & \mathbf{z}\langle\, gh \,:\, g \in \mathfrak{g},\, h \in \mathfrak{h} \,\rangle \;=\; \{\, \textstyle\sum_{i\in[1,k]} g_ih_i \,:\, k \geqslant 0,\, g_i \in \mathfrak{g},\, h_i \in \mathfrak{h} \text{ für } i \in [1,k] \,\} \\
\mathfrak{g}+\mathfrak{h} & := & \{\, g+h \,:\, g \in \mathfrak{g},\, h \in \mathfrak{h} \,\} \\
\mathfrak{g}^{-1} & := & \{\, x \in K \,:\, x\mathfrak{g} \subseteq D \,\}\,.
\end{array}$$

Multiplikation gebrochener Ideale ist assoziativ und kommutativ; cf. betreffende Konvention, angewandt auf Teilmengen von K. Wir können so ohne Klammerung das Produkt mehrerer gebrochener Ideale bilden. Das leere Produkt sei dabei gleich $D = (1)$.

Beachte noch $(x)\mathfrak{g} = x\mathfrak{g}$, $(x)(y) = (xy)$ und $(x)^{-1} = (x^{-1})$ für $x, y \in K^\times$.

Bemerkung 57 *Seien* $\mathfrak{g}, \mathfrak{h} \in \underline{\text{Ideale}}^\times(D)$.

Dann sind auch $\mathfrak{gh}$, $\mathfrak{g} \cap \mathfrak{h}$, $\mathfrak{g} + \mathfrak{h}$, $\mathfrak{g}^{-1} \in \underline{\text{Ideale}}^\times(D)$.

Ist $\mathfrak{g} \subseteq D$, *dann ist* $\mathfrak{g} \in \text{Ideale}^\times(D)$.

Sind bereits $\mathfrak{g}, \mathfrak{h} \in \text{Ideale}^\times(D)$, *dann sind auch* $\mathfrak{gh}$, $\mathfrak{g} \cap \mathfrak{h}$, $\mathfrak{g} + \mathfrak{h} \in \text{Ideale}^\times(D)$.

Beweis. Cf. Aufgabe 28.(1). ▫

Beispiel 58 Sei $D = \mathbf{Z}$; cf. Bemerkung 53.

Es ist $(\frac{3}{5}) + (\frac{9}{2}) = (\frac{3}{5}, \frac{9}{2}) = \frac{1}{10}(6, 45) = \frac{1}{10}(3) = (\frac{3}{10}) \in \underline{\text{Ideale}}^\times(\mathbf{Z})$. Sein Inverses ist $(\frac{10}{3})$.

Lemma 59 *Sei* $\mathfrak{a} \in \text{Ideale}^\times(D)$.

Dann gibt es $n \geqslant 0$ *und* $\mathfrak{p}_i \in \text{Ideale}^\times_{\text{prim}}(D)$ *für* $i \in [1, n]$ *mit*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}\,.$$

Beweis. Bestehe $M \subseteq \text{Ideale}^\times(D)$ aus den Idealen, die der Aussage nicht genügen. Wir haben $M \stackrel{!}{=} \emptyset$ zu zeigen. *Annahme,* nicht. Da D noethersch ist, hat M ein maximales Element $\mathfrak{b}$. Es ist $\mathfrak{b}$ kein Primideal. Es ist $\mathfrak{b} \neq (1)$. Also gibt es Elemente $x_1\,, x_2 \in D$ mit $x_1x_2 \in \mathfrak{b}$, aber $x_1 \notin \mathfrak{b}$ und $x_2 \notin \mathfrak{b}$. Sei $\mathfrak{b}_1 := \mathfrak{b} + (x_1)$. Sei $\mathfrak{b}_2 := \mathfrak{b} + (x_2)$. Dann ist $\mathfrak{b} \subset \mathfrak{b}_1$ und $\mathfrak{b} \subset \mathfrak{b}_2$. Folglich liegen $\mathfrak{b}_1$ und $\mathfrak{b}_2$ in $\text{Ideale}^\times(D) \smallsetminus M$. Seien $n_1 \geqslant 0$ und $\mathfrak{p}_{1,i} \in \text{Ideale}^\times_{\text{prim}}(D)$ für $i \in [1, n_1]$ und $n_2 \geqslant 0$ und $\mathfrak{p}_{2,i} \in \text{Ideale}^\times_{\text{prim}}(D)$ für $i \in [1, n_2]$ mit

$$\begin{aligned} \mathfrak{p}_{1,1}\mathfrak{p}_{1,2} \cdots \mathfrak{p}_{1,n_1} &\subseteq \mathfrak{b}_1 \\ \mathfrak{p}_{2,1}\mathfrak{p}_{2,2} \cdots \mathfrak{p}_{2,n_2} &\subseteq \mathfrak{b}_2 \end{aligned}$$

gewählt. Dann ist

$$\mathfrak{p}_{1,1}\mathfrak{p}_{1,2} \cdots \mathfrak{p}_{1,n_1}\mathfrak{p}_{2,1}\mathfrak{p}_{2,2} \cdots \mathfrak{p}_{2,n_2} \subseteq \mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{b}\,,$$

letzteres, da $x_1x_2 \in \mathfrak{b}$. Also ist $\mathfrak{b} \notin M$ und wir haben einen *Widerspruch.* ▫

Lemma 60 *Sei* $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$. *Dann ist* $D \subset \mathfrak{p}^{-1}$.

Beweis. Es ist $D \subseteq \mathfrak{p}^{-1}$, da $D\mathfrak{p} \subseteq D$. Wir *behaupten* $D \overset{!}{\subset} \mathfrak{p}^{-1}$. Sei $a \in \mathfrak{p}^{\times}$. Sei $n \geqslant 1$ minimal derart, daß wir $\mathfrak{p}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ wählen können mit $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n \subseteq (a)$; cf. Lemma 59.

Da $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n \subseteq (a) \subseteq \mathfrak{p}$, gibt es ein $i \in [1,n]$ mit $\mathfrak{p}_i \subseteq \mathfrak{p}$, wie iterierte Anwendung von Aufgabe 28.(2) zeigt. Sei o.E. $i = 1$. Da D dedekindsch ist und $\mathfrak{p}_1 \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ liegt, ist $\mathfrak{p}_1$ ein maximales Ideal von D. Also ist $\mathfrak{p}_1 = \mathfrak{p}$.

Wegen der Minimalität von n ist $\mathfrak{p}_2\cdots\mathfrak{p}_n \not\subseteq (a)$. Folglich können wir ein $b \in \mathfrak{p}_2\cdots\mathfrak{p}_n \smallsetminus (a)$ wählen. Aus $b \notin (a)$ folgt $a^{-1}b \notin a^{-1}(a) = (1) = D$.

Ferner ist $(a^{-1}b)\mathfrak{p} \subseteq a^{-1}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n \subseteq a^{-1}(a) = (1) = D$. Also ist $a^{-1}b \in \mathfrak{p}^{-1}$. ▫

Lemma 61 *Sei* $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$. *Sei* $\mathfrak{a} \in \mathrm{Ideale}^{\times}(D)$. *Dann ist* $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$.

Beweis. Da $D \subseteq \mathfrak{p}^{-1}$, ist auch $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1}$.

Annahme, es ist $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$.

Sei $x \in \mathfrak{p}^{-1}$ gegeben. Sei $\mathfrak{a} = (\, a_1 \,, \,\ldots\, , \, a_\ell \,)$ für ein $\ell \geqslant 1$ und gewisse $a_i \in D$ für $i \in [1,\ell]$, möglich, da D dedekindsch und also noethersch ist.

Da $x\mathfrak{a} \subseteq \mathfrak{a}$, können wir $xa_i = \sum_{j\in[1,\ell]} s_{i,j}a_j$ schreiben mit $S := (s_{i,j})_{i,j} \in D^{\ell\times\ell}$. Mit $a := (a_i)_i \in D^{\ell\times 1}$ und $T := (x\mathrm{E}_\ell - S) \in K^{\ell\times\ell}$ ist also $Ta = 0$.

Die Cramersche Regel aus Aufgabe 1.(2) gibt ein $T' \in K^{\ell\times\ell}$ mit $T'T = \det(T)\mathrm{E}_\ell$. Also ist $\det(T)a = 0 \in K^{\ell\times 1}$ und folglich $\det(T)a_i = 0$ für $i \in [1,\ell]$. Da $\mathfrak{a} \neq (0)$, gibt es ein $j \in [1,\ell]$ mit $a_j \neq 0$. Aus $\det(T)a_j = 0$ folgt dann $\det(T) = 0$. Daher ist $f(X) := \det(X\mathrm{E}_\ell - S) \in D[X]$ ein normiertes Polynom, für welches $f(x) = \det(x\mathrm{E}_\ell - S) = \det(T) = 0$ ist. Somit ist $x \in \Gamma_K(D)$. Aber $\Gamma_K(D) = D$, da D dedekindsch und also ganzabgeschlossen ist. Also ist $x \in D$.

Dies zeigt $\mathfrak{p}^{-1} \subseteq D$, im *Widerspruch* zu Lemma 60. ▫

Die Argumentation war ähnlich wie bei Lemma 1 zu (3) ⇒ (1).

Korollar 62 *Für* $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ *ist* $\mathfrak{p}\mathfrak{p}^{-1} = D$.

Beweis. Dank Lemma 61 und dank Definition 56.(3) ist $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subseteq D$. Da D dedekindsch ist, ist $\mathfrak{p}$ ein maximales Ideal. Daher muß nun $\mathfrak{p}\mathfrak{p}^{-1} = D$ sein. ▫

Satz 63 (Primidealfaktorzerlegung) *Wir erinnern an D dedekindsch.*
Sei $\mathfrak{a} \in \mathrm{Ideale}^\times(D)$ gegeben.

(1) *Es gibt ein $m \geqslant 0$ und $\mathfrak{p}_i \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$ für $i \in [1,m]$ mit*

$$\mathfrak{a} \;=\; \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m \;.$$

(2) *Sind $m \geqslant 0$ und $\mathfrak{p}_i \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$ für $i \in [1,m]$*
sowie $n \geqslant 0$ und $\mathfrak{q}_i \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$ für $i \in [1,n]$ mit

$$\mathfrak{a} \;=\; \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m \;=\; \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$$

gegeben, dann ist $m = n$, und es gibt ein $\sigma \in \mathrm{S}_m$ mit $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ für $i \in [1,m]$.

Falls D ein Hauptidealbereich ist, kennen wir diese Aussagen aus Aufgabe 2.(3).

Beweis.

Ad (1). Bestehe $M \subseteq \mathrm{Ideale}^\times(D)$ aus den Idealen, die der Aussage nicht genügen. Wir haben $M \stackrel{!}{=} \emptyset$ zu zeigen. *Annahme,* nicht. Da D noethersch ist, hat M ein maximales Element $\mathfrak{b}$. Es ist $\mathfrak{b} \neq (1)$. Sei $\mathfrak{p} \subset D$ ein maximales Ideal, das $\mathfrak{b}$ enthält; cf. Bemerkung 51.(4). Es ist $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$. Es ist

$$\mathfrak{b} \;\overset{\text{L.61}}{\subset}\; \mathfrak{b}\mathfrak{p}^{-1} \;\subseteq\; \mathfrak{p}\mathfrak{p}^{-1} \;\overset{\text{K.62}}{=}\; D \;.$$

Also ist $\mathfrak{b}\mathfrak{p}^{-1} \in \mathrm{Ideale}(D) \smallsetminus M$. Schreibe $\mathfrak{b}\mathfrak{p}^{-1} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$ für ein $n \geqslant 0$ und $\mathfrak{q}_i \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$. Es folgt

$$\mathfrak{b} \;\overset{\text{K.62}}{=}\; \mathfrak{b}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n\mathfrak{p} \;.$$

Ad (2). Sei

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m \;=\; \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$$

gegeben wie in der Aussage. Sei o.E. $m \leqslant n$. Wir führen eine Induktion über $m \geqslant 0$. Im Falle $m = 0$ ist die linke Seite gleich (1), und es folgt $n = 0$, da ansonsten die rechte Seite ein echtes Ideal in D wäre.

Sei nun $m \geqslant 1$. Es ist $\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m \subseteq \mathfrak{p}_m$. Also gibt es ein $i \in [1,n]$ mit $\mathfrak{q}_i \subseteq \mathfrak{p}_m$; cf. Aufgabe 28.(2). O.E. ist $i = n$. Aus D dedekindsch folgt $\mathfrak{q}_n$ maximal, also $\mathfrak{q}_n = \mathfrak{p}_m$ und somit

$$\mathfrak{p}_1\cdots\mathfrak{p}_{m-1} \;\overset{\text{K.62}}{=}\; \mathfrak{p}_1\cdots\mathfrak{p}_{m-1}\mathfrak{p}_m\mathfrak{p}_m^{-1} \;=\; \mathfrak{q}_1\cdots\mathfrak{q}_{n-1}\mathfrak{q}_n\mathfrak{q}_n^{-1} \;\overset{\text{K.62}}{=}\; \mathfrak{q}_1\cdots\mathfrak{q}_{n-1} \;.$$

Induktion zeigt nun, daß $m-1 = n-1$ ist und ein $\rho \in \mathrm{S}_{m-1}$ existiert mit $\mathfrak{q}_{\rho(i)} = \mathfrak{p}_i$ für $i \in [1,m-1]$. Sei nun $\sigma(i) := \rho(i)$ für $i \in [1,m-1]$ und $\sigma(m) := m = n$. ▫

Korollar 64 *Es ist* $\underline{\text{Ideale}}^\times(D)$ *eine abelsche Gruppe mit der in Definition* 56.(3) *eingeführten Multiplikation gebrochener Ideale.*

Dabei ist für $\mathfrak{g} \in \underline{\text{Ideale}}^\times(D)$ *das multiplikativ Inverse durch* $\mathfrak{g}^{-1}$ *im Sinne von Definition* 56.(3) *gegeben.*

Beweis. Zeigen wir die Gruppeneigenschaft. Die Multiplikation ist kommutativ und assoziativ. Es ist (1) ein neutrales Element.

Es bleibt zu zeigen, daß zu jedem gegebenen $\mathfrak{g} \in \underline{\text{Ideale}}^\times(D)$ ein Inverses existiert. Schreibe $\mathfrak{g} = x\mathfrak{a}$ mit $x \in K^\times$ und $\mathfrak{a} \in \text{Ideale}^\times(D)$. Schreibe $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ mit $m \geqslant 0$ und $\mathfrak{p}_i \in \text{Ideale}^\times_{\text{prim}}(D)$ für $i \in [1, m]$; cf. Satz 63.(1). Es wird

$$\mathfrak{g} \cdot \left(x^{-1}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}\right) \;=\; x\mathfrak{p}_1 \cdots \mathfrak{p}_m \cdot x^{-1}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1} \;\overset{\text{K. 62}}{=}\; (1)\ .$$

Bleibt zu zeigen, daß dieses multiplikativ Inverse gleich $\mathfrak{g}^{-1}$ im Sinne von Definition 56.(3) ist.

Es ist $\mathfrak{g}^{-1} = (x\mathfrak{a})^{-1} = x^{-1}\mathfrak{a}^{-1}$, da für $y \in K$ genau dann $y \in (x\mathfrak{a})^{-1}$ liegt, wenn $yx\mathfrak{a} \subseteq (1)$, i.e. $yx \in \mathfrak{a}^{-1}$, i.e. $y \in x^{-1}\mathfrak{a}^{-1}$ liegt.

Aus $\mathfrak{a} \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_m \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1} \subseteq (1)$ folgt $\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1} \subseteq \mathfrak{a}^{-1}$.

Aus $\mathfrak{a}^{-1} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{a}^{-1} \cdot \mathfrak{a} \subseteq (1)$ folgt durch Multiplikation mit $\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$ dank Korollar 62, daß $\mathfrak{a}^{-1} \subseteq \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$ ist.

Zusammen ist $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$ und somit $\mathfrak{g}^{-1} = x^{-1}\mathfrak{a}^{-1} = x^{-1}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$, wie noch zu zeigen blieb. ▫

Lemma 65 *Schreibe* $P := \text{Ideale}^\times_{\text{prim}}(D)$.

Sei

$$\mathbf{Z}^{\oplus P} \;:=\; \{\, (\gamma_\mathfrak{p})_{\mathfrak{p}\in P} \,:\, \gamma_\mathfrak{p} \in \mathbf{Z} \text{ für } \mathfrak{p} \in P \text{ und } \{\, \mathfrak{p} \in P \,:\, \gamma_\mathfrak{p} \neq 0 \,\} \text{ endlich} \,\}\ .$$

Wir haben einen Isomorphismus abelscher Gruppen

$$\begin{array}{rcl} \mathbf{Z}^{\oplus P} & \xrightarrow[\sim]{\varphi} & \underline{\text{Ideale}}^\times(D) \\ (\gamma_\mathfrak{p})_{\mathfrak{p}\in P} & \longmapsto & \prod_{\mathfrak{p}\in P,\, \gamma_\mathfrak{p}\neq 0} \mathfrak{p}^{\gamma_\mathfrak{p}} \end{array}$$

Für $(\gamma_\mathfrak{p})_{\mathfrak{p}\in P} \in \mathbf{Z}^{\oplus P}$ *schreiben wir dann auch* $\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_\mathfrak{p}} := \prod_{\mathfrak{p}\in P,\, \gamma_\mathfrak{p}\neq 0} \mathfrak{p}^{\gamma_\mathfrak{p}}$.

Sei

$$(\mathrm{v}_\mathfrak{p}(\mathfrak{g}))_{\mathfrak{p}\in P} \;:=\; \varphi^{-1}(\mathfrak{g})\ .$$

I.e.

$$\begin{array}{rcll} \mathfrak{g} & = & \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{g})} & \textit{für } \mathfrak{g} \in \underline{\text{Ideale}}^\times(D) \\ \gamma_\mathfrak{q} & = & \mathrm{v}_\mathfrak{q}(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_\mathfrak{p}}) & \textit{für } (\gamma_\mathfrak{p})_{\mathfrak{p}\in P} \in \mathbf{Z}^{\oplus P} \textit{ und } \mathfrak{q} \in P\ . \end{array}$$

Es heißt $\mathrm{v}_\mathfrak{p}(\mathfrak{g})$ *die* Bewertung *von* $\mathfrak{g}$ *bei* $\mathfrak{p}$.

Wir setzen noch $\mathrm{v}_{\mathfrak{p}}((0)) := \infty$ *und* $\mathrm{v}_{\mathfrak{p}}(x) := \mathrm{v}_{\mathfrak{p}}((x))$ *für* $x \in K$ *und* $\mathfrak{p} \in P$.

Ist $\mathfrak{p} \in P$ *ein Hauptideal, also* $\mathfrak{p} = (p)$ *für ein Primelement* $p \in D^\times$, *dann schreiben wir auch* $\mathrm{v}_p := \mathrm{v}_{(p)} = \mathrm{v}_{\mathfrak{p}}$.

Cf. auch Aufgabe 2.(4).

Beweis. Für $(\gamma_{\mathfrak{p}})_{\mathfrak{p}}$, $(\beta_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbf{Z}^{\oplus P}$ ist

$$\varphi\big((\gamma_{\mathfrak{p}})_{\mathfrak{p}}+(\beta_{\mathfrak{p}})_{\mathfrak{p}}\big) \;=\; \varphi\big((\gamma_{\mathfrak{p}}+\beta_{\mathfrak{p}})_{\mathfrak{p}}\big) \;=\; \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_{\mathfrak{p}}+\beta_{\mathfrak{p}}} \;=\; \big(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_{\mathfrak{p}}}\big)\cdot\big(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\beta_{\mathfrak{p}}}\big) \;=\; \varphi\big((\gamma_{\mathfrak{p}})_{\mathfrak{p}}\big)\cdot\varphi\big((\beta_{\mathfrak{p}})_{\mathfrak{p}}\big) \;.$$

Also ist φ ein Morphismus abelscher Gruppen.

Wir *behaupten* die Injektivität von φ. Sei $(\gamma_{\mathfrak{p}})_{\mathfrak{p}\in P} \in \mathbf{Z}^{\oplus P}$ mit $\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_{\mathfrak{p}}} = (1)$ gegeben. Wir haben $\gamma_{\mathfrak{p}} \stackrel{!}{=} 0$ für $\mathfrak{p} \in P$ zu zeigen. Es ist

$$\prod_{\mathfrak{p}\in P,\ \gamma_{\mathfrak{p}}>0} \mathfrak{p}^{\gamma_{\mathfrak{p}}} \;=\; \prod_{\mathfrak{p}\in P,\ \gamma_{\mathfrak{p}}<0} \mathfrak{p}^{-\gamma_{\mathfrak{p}}} \;.$$

Gäbe es ein $\mathfrak{q} \in P$ mit $\gamma_{\mathfrak{q}} > 0$, dann würde $\mathfrak{q}$ in der linken, nicht aber in der rechten Seite als Faktor auftreten, im *Widerspruch* zu Satz 63.(2). *Gäbe* es ein $\mathfrak{q} \in P$ mit $\gamma_{\mathfrak{q}} < 0$, dann würde $\mathfrak{q}$ in der rechten, nicht aber in der linken Seite als Faktor auftreten, im *Widerspruch* zu Satz 63.(2). Also ist $\gamma_{\mathfrak{p}} = 0$ für $\mathfrak{p} \in P$.

Wir *behaupten* die Surjektivität von φ. Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(D)$ gegeben. Schreibe $\mathfrak{g} = \frac{1}{d}\mathfrak{a}$ mit $d \in D^\times$ und $\mathfrak{a} \in \mathrm{Ideale}^\times(D)$. Schreibe $(d) =: \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\delta_{\mathfrak{p}}}$ und $\mathfrak{a} =: \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$ mit $(\delta_{\mathfrak{p}})_{\mathfrak{p}}$, $(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbf{Z}^{\oplus P}$, wobei stets $\delta_{\mathfrak{p}}$, $\alpha_{\mathfrak{p}} \geqslant 0$; cf. Satz 63.(1). Dann wird $(\alpha_{\mathfrak{p}} - \delta_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbf{Z}^{\oplus P}$ und

$$\mathfrak{g} \;=\; (d)^{-1}\cdot\mathfrak{a} \;=\; \big(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{-\delta_{\mathfrak{p}}}\big)\cdot\big(\prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_{\mathfrak{p}}}\big) \;=\; \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\alpha_{\mathfrak{p}}-\delta_{\mathfrak{p}}} \;=\; \varphi\big((\alpha_{\mathfrak{p}} - \delta_{\mathfrak{p}})_{\mathfrak{p}}\big) \;.$$

□

Bemerkung 66 *Schreibe* $P := \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$.

(1) *Für* $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(D)$ *ist genau dann* $\mathfrak{g} \in \mathrm{Ideale}^\times(D)$, *wenn* $\mathrm{v}_{\mathfrak{p}}(\mathfrak{g}) \geqslant 0$ *ist für* $\mathfrak{p} \in P$.

(2) *Für* $x \in K$ *ist genau dann* $x \in D$, *wenn* $\mathrm{v}_{\mathfrak{p}}(x) \geqslant 0$ *ist für* $\mathfrak{p} \in P$.

(3) *Für* $u \in K$ *ist genau dann* $u \in \mathrm{U}(D)$, *wenn* $\mathrm{v}_{\mathfrak{p}}(u) = 0$ *ist für* $\mathfrak{p} \in P$.

Beweis.

Ad (1). Ist $\mathfrak{g} \in \mathrm{Ideale}^\times(D)$, dann können wir $\mathfrak{g} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\gamma_{\mathfrak{p}}}$ schreiben mit $\gamma_{\mathfrak{p}} \geqslant 0$ stets; cf. Satz 63.(1). Dann ist $\mathrm{v}_{\mathfrak{p}}(\mathfrak{g}) = \gamma_{\mathfrak{p}}$ für $\mathfrak{p} \in P$; cf. Lemma 65.

Ist umgekehrt $\mathrm{v}_{\mathfrak{p}}(\mathfrak{g}) \geqslant 0$ für $\mathfrak{p} \in P$, dann ist $\mathfrak{g} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{g})} \subseteq D$, insbesondere $\mathfrak{g} \in \mathrm{Ideale}^\times(D)$; cf. Lemma 65, Bemerkung 57.

Ad (2). O.E. ist $x \in K^\times$. Die Aussage ergibt sich aus (1) für $\mathfrak{g} = (x)$.

Ad (3). O.E. ist $u \in K^\times$. Ist $u \in \mathrm{U}(D)$, dann ist $(u) = (1)$ und also $\mathrm{v}_\mathfrak{p}(u) = 0$ für $\mathfrak{p} \in P$. Ist umgekehrt $\mathrm{v}_\mathfrak{p}(u) = 0$ für $\mathfrak{p} \in P$ vorausgesetzt, dann ist auch $\mathrm{v}_\mathfrak{p}(u^{-1}) = -\mathrm{v}_\mathfrak{p}(u) = 0$ für $\mathfrak{p} \in P$, somit $u \in D$ und $u^{-1} \in D$ und also $u \in \mathrm{U}(D)$. ▫

Definition 67 Schreibe $\underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D) := \{\, (x) \,:\, x \in K^\times \,\} \subseteq \underline{\mathrm{Ideale}}^\times(D)$ für die Teilmenge der gebrochenen Hauptideale.

Sei daran erinnert, daß $\underline{\mathrm{Ideale}}^\times(D)$ eine abelsche Gruppe ist bezüglich der Multiplikation gebrochener Ideale; cf. Korollar 64.

Da $(1) \in \underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D)$ und da für $x, y \in K^\times$ sich $(x)(y)^{-1} = (xy^{-1}) \in \underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D)$ ergibt, ist $\underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D) \leqslant \underline{\mathrm{Ideale}}^\times(D)$.

Die Faktorgruppe

$$\mathrm{Cl}(D) \;:=\; \underline{\mathrm{Ideale}}^\times(D)/\underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D)$$

heißt *Klassengruppe* von D.

Für $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(D)$ schreiben wir $[\mathfrak{g}] := \mathfrak{g}\,\underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D) \in \mathrm{Cl}(D)$ für die Restklasse von $\mathfrak{g}$ in der Klassengruppe.

> Ist $K|\mathbf{Q}$ eine endliche Körpererweiterung, i.e. K ein Zahlkörper, so wird in der Literatur auch $\mathrm{Cl}(K) := \mathrm{Cl}(\mathcal{O}_K)$ geschrieben.

Beispiel 68 In Aufgabe 27.(1) wurde $\mathfrak{a} \in \mathrm{Ideale}^\times(\mathbf{Z}[\sqrt{-5}])$ mit $[\mathfrak{a}] \neq 1$, aber $[\mathfrak{a}]^2 = [\mathfrak{a}^2] = 1$ gefunden. Also hat $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathbf{Z}[\sqrt{-5}])$ die Ordnung 2.

Bemerkung 69

(1) *Es ist* $\mathrm{Cl}(D) \simeq 1$ *genau dann, wenn* D *ein Hauptidealbereich ist.*

(2) *Wir haben die exakte Sequenz abelscher Gruppen*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{U}(D) & \longrightarrow & K^\times & \longrightarrow & \underline{\mathrm{Ideale}}^\times(D) & \longrightarrow & \mathrm{Cl}(D) \longrightarrow 1 \\ & & d & \longmapsto & d & & \mathfrak{g} & \longmapsto & [\mathfrak{g}]\,. \\ & & & & x & \longmapsto & (x) & & \end{array}$$

> *Dies besage, daß das Bild jedes auftretenden Morphismus gleich dem Kern des nachfolgenden ist.*

Beweis.

Ad (1). Es ist $\mathrm{Cl}(D) \simeq 1$ genau dann, wenn $\underline{\mathrm{Ideale}}^\times_{\mathrm{Haupt}}(D) = \underline{\mathrm{Ideale}}^\times(D)$ ist, i.e. wenn jedes gebrochene Ideal von D ein gebrochenes Hauptideal ist.

Dies ist der Fall, wenn D ein Hauptidealbereich ist.

Ist umgekehrt $\mathrm{Cl}(D) \simeq 1$ vorausgesetzt, dann ist jedes Ideal von D, o.E. ungleich (0), ein gebrochenes Hauptideal von D, welches in D liegt. Insbesondere liegt sein Erzeuger in D, sodaß es ein Hauptideal ist.

Ad (2). Zu zeigen ist nur, daß für $x \in K^\times$ genau dann $(x) = (1)$ ist, wenn $x \in \mathrm{U}(D)$ liegt. Es ist $(x) = (1)$ genau dann, wenn es ein $d \in D$ mit $xd = 1$ und ein $e \in D$ mit $x = 1 \cdot e$ gibt. Es folgt $x \in D$ und $xd = 1$, also $x \in \mathrm{U}(D)$. ▫

2.3 Lokale Betrachtungen

2.3.1 Lokale Charakterisierung von Dedekindbereichen

Lemma 70 *Sei A ein Integritätsbereich. Schreibe $K := \mathrm{Quot}(A)$.*

Sei $L|K$ eine Körpererweiterung.

Sei $S \subseteq A^\times$ mit $1 \in S$ und mit $st \in S$ für $s, t \in S$ gegeben.

Wir betrachten den Teilring $S^{-1}A = \{ \frac{a}{s} : a \in A,\ s \in S \} \subseteq K$ wie in Aufgabe 10.(1).

(1) *Sei $\mathfrak{b} \in \mathrm{Ideale}(S^{-1}A)$. Es ist $S^{-1}(\mathfrak{b} \cap A) = \mathfrak{b}$.*

(2) *Ist A noethersch, dann ist auch $S^{-1}A$ noethersch.*
Gibt es zudem ein $n \geqslant 0$ derart, daß jedes Ideal von A von n Elementen erzeugt ist, dann ist auch jedes Ideal von $S^{-1}A$ von n Elementen erzeugt.

(3) *Ist A ein Hauptidealbereich, dann ist auch $S^{-1}A$ ein Hauptidealbereich.*

(4) *Es ist $S^{-1}\Gamma_L(A) = \Gamma_L(S^{-1}A)$.*

(5) *Ist A ganzabgeschlossen, dann ist auch $S^{-1}A$ ganzabgeschlossen.*

(6) *Ist A dedekindsch, dann ist auch $S^{-1}A$ dedekindsch.*

Beweis.

Ad (1).

Zu $\overset{!}{\subseteq}$. Ist $x = \frac{x}{1} \in \mathfrak{b} \cap A$ und $s \in S$, dann ist $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in \mathfrak{b}$, da $\frac{1}{s} \in S^{-1}A$ und $\frac{x}{1} \in \mathfrak{b}$.

Zu $\overset{!}{\supseteq}$. Ist $\frac{y}{t} \in \mathfrak{b}$ mit $y \in A$ und $t \in S$, dann ist $y = \frac{y}{1} = \frac{t}{1} \cdot \frac{y}{t} \in A \cap \mathfrak{b}$. Also ist $\frac{y}{t} \in S^{-1}(\mathfrak{b} \cap A)$.

Ad (2). Sei $\mathfrak{b} \in \mathrm{Ideale}(S^{-1}A)$. Wir haben zu zeigen, daß $\mathfrak{b}$ endlich erzeugt ist. Da A noethersch ist und da $\mathfrak{b} \cap A \in \mathrm{Ideale}(A)$ liegt, können wir $\mathfrak{b} \cap A = (\, x_1 \,, \,\ldots\, , \, x_m \,)$ schreiben mit einem $m \geqslant 0$ und gewissen $x_i \in A$ mit $i \in [1, m]$. Also ist

$$\mathfrak{b} \overset{(1)}{=} S^{-1}(\mathfrak{b} \cap A) \;=\; \Big\{ \frac{1}{s} \sum_{i \in [1,m]} a_i x_i \;:\; s \in S \text{ und } a_i \in A \text{ für } i \in [1,m] \Big\} \;=\; (\, x_1 \,, \,\ldots\, , \, x_m \,)\,,$$

wobei letzteres Idealerzeugnis nun in $S^{-1}A$ zu lesen ist, und wobei letztere Gleichheit in der Richtung $\subseteq$ direkt folgt, in der Richtung $\supseteq$ daher rührt, daß x_i in der linken Seite liegt für $i \in [1, m]$.

Ist nun jedes Ideal von A von n Elementen erzeugt, dann ist stets $m = n$ wählbar und also auch jedes Ideal von $S^{-1}A$ von n Elementen erzeugt.

Ad (3). Dies wird von der Zusatzaussage in (2) mit $n = 1$ geliefert.

Ad (4). Ist $z \in \Gamma_L(S^{-1}A)$, dann gibt es $f(X) \in (S^{-1}A)[X]$ normiert mit $f(z) = 0$. Nach Multiplikation mit einem gemeinsamen Nenner können wir

$$f(X) \;=\; \frac{1}{s}\big(sX^n + \sum_{i\in[0,n-1]} a_i X^i\big)$$

schreiben, wobei $n := \deg(f)$, $s \in S$ und $a_i \in A$ für $i \in [0, n-1]$. Folglich ist

$$(sz)^n + \sum_{i\in[0,n-1]} (a_i s^{n-i-1})(sz)^i \;=\; 0\,.$$

Also ist $sz \in \Gamma_L(A)$, und daher $z = \frac{sz}{s} \in S^{-1}\Gamma_L(A)$.

Ist $w \in S^{-1}\Gamma_L(A)$, dann können wir $w = \frac{u}{s}$ schreiben mit $s \in S$ und $u \in \Gamma_L(A)$. Es gibt $g(X) \in A[X]$ normiert mit $g(u) = 0$. Schreibe $g(X) = X^n + \sum_{i\in[0,n-1]} b_i X^i$ mit $b_i \in A$ für $i \in [0, n-1]$. Dann ist

$$\Big(\frac{u}{s}\Big)^n + \sum_{i\in[0,n-1]} \frac{b_i}{s^{n-i}}\Big(\frac{u}{s}\Big)^i \;=\; 0\,.$$

Also ist $w = \frac{u}{s} \in \Gamma_L(S^{-1}A)$.

Ad (5). Es ist $K = \mathrm{Quot}(S^{-1}A)$; cf. Aufgabe 11.(2). Ist A ganzabgeschlossen, dann wird

$$\Gamma_K(S^{-1}A) \;\overset{(4)}{=}\; S^{-1}\Gamma_K(A) = S^{-1}A\,.$$

Also ist auch $S^{-1}A$ ganzabgeschlossen.

Ad (6). Sei A dedekindsch; cf. Definition 50. Dann ist der Integritätsbereich $S^{-1}A$ noethersch nach (2) und ganzabgeschlossen nach (5). Da die Bijektion aus Aufgabe 10.(1) von der Menge der Primideale von A, die leeren Schnitt mit S haben, zur Menge der Primideale von $S^{-1}A$ inklusionserhaltend ist und da in A keine Primideale $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3$ existieren, ist das in $S^{-1}A$ auch nicht der Fall. Somit ist jedes $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(S^{-1}A)$ maximal. Insgesamt ist $S^{-1}A$ dedekindsch. ▫

Lemma 71 (Approximation) *Sei D ein Dedekindbereich. Schreibe $K := \mathrm{Quot}(D)$.*

Sei $n \geqslant 0$ gegeben. Seien $\mathfrak{p}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$, $\gamma_i \in \mathbf{Z}$ und $y_i \in K$ gegeben für $i \in [1,n]$. Sei dabei $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i, j \in [1,n]$ mit $i \neq j$.

Dann gibt es ein $x \in K^{\times}$ mit

$$\begin{array}{lcll} \mathrm{v}_{\mathfrak{p}_i}(x - y_i) & = & \gamma_i & \text{für } i \in [1,n] \\ \mathrm{v}_{\mathfrak{q}}(x) & \geqslant & 0 & \text{für } \mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D) \smallsetminus \{\, \mathfrak{p}_i \,:\, i \in [1,n] \,\}\,. \end{array}$$

Ist $\gamma_i \geqslant 0$ und $y_i \in D$ für $i \in [1,n]$, dann findet sich ein solches x bereits in $D^{\times}$.

> Könnte man anstelle des $\geqslant$ ein $=$ schreiben, dann fände man insbesondere im Fall $n = 1$, $y_1 = 0$ und $\gamma_1 = 1$ ein Element $x \in D$, für welches (x) überall dieselbe Bewertung hat wie $\mathfrak{p}_1$, für welches also nach Lemma 65 auch $(x) = \mathfrak{p}_1$ gälte – es folgte, daß in D alle Primideale und damit überhaupt alle Ideale Hauptideale wären. Das ist i.a. aber nicht der Fall; cf. Beispiele 55 und 68.

Beweis.

Vorbemerkung. Für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ und $k \geqslant 0$ ist $\mathfrak{p}^{k+1} \subset \mathfrak{p}^k$, da wegen Satz 63.(2) keine Gleichheit gelten kann.

Beachte auch Aufgabe 29.(1).

Reduktionsschritt. Sei $s \in D^{\times}$ so, daß $sy_i \in D$ und $s\mathfrak{p}_i^{\gamma_i} \subseteq D$ liegen für $i \in [1,n]$. Sei $(s) =: \prod_{i \in [1,m]} \mathfrak{p}_i^{\sigma_i}$ mit $m \geqslant n$, mit $\mathfrak{p}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ auch für $i \in [n+1,m]$ und mit $\sigma_i \geqslant 0$ für $i \in [1,m]$. Setze $\gamma_i := 0$ und $y_i := 0$ für $i \in [n+1,m]$. Es ist $\sigma_i + \gamma_i \geqslant 0$ für $i \in [1,m]$.

Finden wir ein $\tilde{x} \in D^{\times}$ mit $\mathrm{v}_{\mathfrak{p}_i}(\tilde{x} - sy_i) = \gamma_i + \sigma_i$ für $i \in [1,m]$, dann ist mit $x := \tilde{x}/s \in K^{\times}$ auch $\mathrm{v}_{\mathfrak{p}_i}(x - y_i) = \mathrm{v}_{\mathfrak{p}_i}((\tilde{x} - sy_i)/s) = \gamma_i$ für $i \in [1,m]$. Insbesondere also für $i \in [1,n]$. Für $i \in [n+1,m]$ liest sich die Gleichung als $\mathrm{v}_{\mathfrak{p}_i}(x) = 0$. Für $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ mit $\mathfrak{q} \notin \{\, \mathfrak{p}_i \,:\, i \in [1,m] \,\}$ ist $\mathrm{v}_{\mathfrak{q}}(x) = \mathrm{v}_{\mathfrak{q}}(\tilde{x}) - \mathrm{v}_{\mathfrak{q}}(s) = \mathrm{v}_{\mathfrak{q}}(\tilde{x}) \geqslant 0$.

Beweis im reduzierten Fall. Dank Reduktionsschritt dürfen wir o.E. $y_i \in D$ und $\gamma_i \geqslant 0$ für $i \in [1,n]$ annehmen, sofern wir dann $x \in D^{\times}$ suchen.

O.E. ist $n \geqslant 1$. Wir haben den surjektiven Ringmorphismus

$$\begin{array}{ccc} D & \longrightarrow & \prod_{i \in [1,n]} D/\mathfrak{p}_i^{\gamma_i+1} \\ d & \longmapsto & (d + \mathfrak{p}_i^{\gamma_i+1})_i \end{array}$$

gemäß Aufgabe 26.(2). Wähle ein $z_i \in \mathfrak{p}_i^{\gamma_i} \smallsetminus \mathfrak{p}_i^{\gamma_i+1}$ für $i \in [1,n]$, möglich dank Vorbemerkung. Sei $x \in D$ ein Urbild von $(y_i + z_i + \mathfrak{p}_i^{\gamma_i+1})_i \in \prod_{i \in [1,n]} D/\mathfrak{p}_i^{\gamma_i+1}$. Es ist $x \neq 0$ erreichbar durch eventuelle Addition eines Elements aus $\prod_{i \in [1,n]} \mathfrak{p}_i^{\gamma_i+1}$.

Sei $i \in [1,n]$. Es ist $x \equiv_{\mathfrak{p}_i^{\gamma_i+1}} y_i + z_i$. Zum einen folgt $x - y_i \equiv_{\mathfrak{p}_i^{\gamma_i+1}} z_i \equiv_{\mathfrak{p}_i^{\gamma_i}} 0$, also $\mathrm{v}_{\mathfrak{p}_i}(x - y_i) \geqslant \gamma_i$. Zum anderen folgt $x - y_i \equiv_{\mathfrak{p}_i^{\gamma_i+1}} z_i \not\equiv_{\mathfrak{p}_i^{\gamma_i+1}} 0$, also $\mathrm{v}_{\mathfrak{p}_i}(x - y_i) \leqslant \gamma_i$. Zusammen ist $\mathrm{v}_{\mathfrak{p}_i}(x - y_i) = \gamma_i$. ▫

Lemma 72 *Sei D ein Dedekindbereich, für welchen $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ endlich ist. Dann ist D ein Hauptidealbereich.*

Beweis. Sei $\mathfrak{a} \in \mathrm{Ideale}^{\times}(D)$. Wir haben zu zeigen, daß $\mathfrak{a}$ ein Hauptideal ist. Sei $n := |\,\mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)|$ und $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(D) =: \{\,\mathfrak{p}_i \,:\, i \in [1,n]\,\}$. Nach Lemma 71 gibt es ein $x \in D^{\times}$ mit $\mathrm{v}_{\mathfrak{p}_i}(x) = \mathrm{v}_{\mathfrak{p}_i}(\mathfrak{a})$ für $i \in [1,n]$. Also ist $(x) = \mathfrak{a}$; cf. Lemma 65. ▫

Definition 73 Sei R ein Hauptidealbereich.

Es heißt R ein *diskreter Bewertungsring*, falls $|\,\mathrm{Ideale}^{\times}_{\mathrm{prim}}(R)| = 1$ ist.

Diesenfalls ist $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(R) = \{(\pi)\}$ mit einem geeigneten $\pi \in R^{\times}$. Es heißt $\mathrm{v}_{(\pi)} = \mathrm{v}_{\pi}$ die *(diskrete) Bewertung* auf R; cf. Aufgabe 2.(5).

Bemerkung 74 *Sei D ein Dedekindbereich. Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$.*

Es ist $D_{\mathfrak{p}}$ ein diskreter Bewertungsring.

Beweis. Es ist $D_{\mathfrak{p}}$ ein Dedekindbereich; cf. Lemma 70.(6). Es ist $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(D_{\mathfrak{p}}) = \{\mathfrak{p}_{\mathfrak{p}}\}$; cf. Aufgabe 10.(2). Insbesondere ist $D_{\mathfrak{p}}$ ein Hauptidealbereich; cf. Lemma 72. ▫

E.g. für $p \in \mathbf{Z}_{>0}$ prim ist so $\mathbf{Z}_{(p)} = \{\,\frac{a}{s} \in \mathbf{Q} \,:\, a \in \mathbf{Z},\ s \in \mathbf{Z},\ s \not\equiv_p 0\,\}$ ein diskreter Bewertungsring mit den Primidealen (0) und (p). Wir haben den Körperisomorphismus $\mathbf{F}_p \xrightarrow{\sim} \mathbf{Z}_{(p)}/(p)$, $1 \longmapsto 1 + (p)$, entlang dem wir identifizieren; cf. Aufgabe 10.(2).

Bemerkung 75 *Sei R ein diskreter Bewertungsring mit Primelement $\pi \in R^{\times}$. Sei $K := \mathrm{Quot}(R)$.*

Es ist

$$\begin{aligned}
R^{\times} &= \{\,\pi^k e \,:\, k \in \mathbf{Z}_{\geqslant 0},\ e \in \mathrm{U}(R)\,\} \\
K^{\times} &= \{\,\pi^k e \,:\, k \in \mathbf{Z},\ e \in \mathrm{U}(R)\,\} \\
\mathrm{U}(R) &= \{\,x \in R \,:\, \mathrm{v}_{\pi}(x) = 0\,\} \\
(\pi) &= \{\,x \in R \,:\, \mathrm{v}_{\pi}(x) \geqslant 1\,\} \\
\mathrm{Ideale}^{\times}(R) &= \{\,(\pi^k) \,:\, k \in \mathbf{Z}_{\geqslant 0}\,\} \\
\underline{\mathrm{Ideale}}^{\times}(R) &= \{\,(\pi^k) \,:\, k \in \mathbf{Z}_{\geqslant 0}\,\}\,.
\end{aligned}$$

Beweis. Jedes Element von $R^{\times}$ ist von der Form $\pi^k e$ mit einem $e \in \mathrm{U}(R)$ und mit $k = \mathrm{v}_{\pi}(\pi^k e) \in \mathbf{Z}_{\geqslant 0}$; cf. Aufgabe 2.(4).

Folglich ist jedes Element von $K^{\times}$ von der Form $\pi^k e$ mit einem $e \in \mathrm{U}(R)$ und einem $k \in \mathbf{Z}$.

Ist $k \geqslant 0$ und $e \in \mathrm{U}(R)$, dann ist $\pi^k e \in \mathrm{U}(R)$ genau dann, wenn $k = 0$ ist, da es für $k \geqslant 1$ in $(\pi) \subset R$ liegt.

Jedes Element von $\mathrm{Ideale}^{\times}(R)$ ist von der Form $(\pi^k e)$ für ein $k \in \mathbf{Z}_{\geqslant 0}$ und ein $e \in \mathrm{U}(R)$, was $(\pi^k e) = (\pi^k)$ nach sich zieht.

Jedes Element von $\underline{\text{Ideale}}^\times(R)$ ist von der Form $(\pi^k e)$ für ein $k \in \mathbf{Z}$ und ein $e \in \mathrm{U}(R)$, was $(\pi^k e) = (\pi^k)$ nach sich zieht. ▫

Bemerkung 76 *Sei D ein Dedekindbereich. Schreibe $K := \mathrm{Quot}(D)$.*

Sei $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$. Es ist

$$D_\mathfrak{p} \;=\; \{\, x \in K \,:\, \mathrm{v}_\mathfrak{p}(x) \geqslant 0 \,\}\,.$$

Insbesondere ist $D = \bigcap_{\mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)} D_\mathfrak{q}$, gebildet in K.

Beweis. Zeigen wir $D_\mathfrak{p} \overset{!}{=} \{\, x \in K \,:\, \mathrm{v}_\mathfrak{p}(x) \geqslant 0 \,\}$.

Ad $\overset{!}{\subseteq}$. Es ist $\mathrm{v}_\mathfrak{p}(0) = \infty \geqslant 0$.

Für $d \in D^\times$ und $s \in D \smallsetminus \mathfrak{p}$ ist $\mathrm{v}_\mathfrak{p}(d) \geqslant 0$ und $\mathrm{v}_\mathfrak{p}(s) = 0$, denn $\mathrm{v}_\mathfrak{p}(s) \geqslant 1$ hätte $(s) \subseteq \mathfrak{p}$ zur Folge. Also ist $\mathrm{v}_\mathfrak{p}(\frac{d}{s}) = \mathrm{v}_\mathfrak{p}(d) - \mathrm{v}_\mathfrak{p}(s) \geqslant 0$; cf. Aufgabe 29.(2).

Ad $\overset{!}{\supseteq}$. Es ist $0 \in D_\mathfrak{p}$.

Sei $x \in K^\times$ mit $\mathrm{v}_\mathfrak{p}(x) \geqslant 0$ gegeben. Wir können $x = \frac{u}{v}$ schreiben mit $u,\, v \in D^\times$. Es ist $0 \leqslant \mathrm{v}_\mathfrak{p}(x) = \mathrm{v}_\mathfrak{p}(u) - \mathrm{v}_\mathfrak{p}(v)$. Wähle $y \in K^\times$ mit $\mathrm{v}_\mathfrak{p}(y) = -\mathrm{v}_\mathfrak{p}(v)$ und mit $\mathrm{v}_\mathfrak{q}(y) \geqslant 0$ für $\mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D) \smallsetminus \{\mathfrak{p}\}$; cf. Lemma 71. Dann ist $\mathrm{v}_\mathfrak{p}(uy) \geqslant \mathrm{v}_\mathfrak{p}(vy) = 0$ und $\mathrm{v}_\mathfrak{q}(uy),\, \mathrm{v}_\mathfrak{q}(vy) \geqslant 0$ für $\mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D) \smallsetminus \{\mathfrak{p}\}$ und also $uy,\, vy \in D^\times$; cf. Bemerkung 66.(2). Aus $\mathrm{v}_\mathfrak{p}(vy) = 0$ folgt ferner $vy \in D \smallsetminus \mathfrak{p}$. Somit ist $x = \frac{uy}{vy} \in D_\mathfrak{p}$.

Die Aussage über den Schnitt folgt nun mit Bemerkung 66.(2). ▫

Die Aussage über den Schnitt brauchen wir in noch etwas größerer Allgemeinheit:

Lemma 77 *Sei A ein noetherscher Integritätsbereich. Schreibe $K := \mathrm{Quot}(A)$.*

Sei M die Menge der maximalen Ideale von A.

Für $\mathfrak{a} \in \mathrm{Ideale}(A)$ ist $\mathfrak{a} = \bigcap_{\mathfrak{m} \in M} \mathfrak{a}_\mathfrak{m}$, gebildet in K

Bei Verzicht auf Noetherzität ist die Aussage dank Zorns Lemma immer noch richtig.

Beweis. Zu zeigen ist nur $\overset{!}{\supseteq}$. Sei $x \in K$ in $\mathfrak{a}_\mathfrak{m}$ gelegen für alle $\mathfrak{m} \in M$. Wir haben $x \in \mathfrak{a}$ zu zeigen.

Annahme, es ist $x \notin \mathfrak{a}$. Sei $\mathfrak{b} := \{\, y \in A \,:\, yx \in \mathfrak{a} \,\}$. Es ist $\mathfrak{b}$ ein Ideal in A, da $0 \in \mathfrak{b}$ und da für $s,\, s' \in A$ und $y,\, y' \in \mathfrak{b}$ sich $(sy + s'y')x = s(yx) + s'(y'x) \in \mathfrak{a}$ ergibt. Es ist $1 \notin \mathfrak{b}$, also $\mathfrak{b} \subset A$. Folglich gibt es ein maximales Ideal $\mathfrak{n} \subset A$ mit $\mathfrak{b} \subseteq \mathfrak{n}$; cf. Bemerkung 51.(4). Nun ist aber $x \in \mathfrak{a}_\mathfrak{n}$. Also können wir $x = \frac{a}{t}$ schreiben mit $a \in \mathfrak{a}$ und $t \in A \smallsetminus \mathfrak{n}$. Folglich ist $tx = a \in \mathfrak{a}$. Also ist $t \in \mathfrak{b} \smallsetminus \mathfrak{n}$, im *Widerspruch* zu $\mathfrak{b} \subseteq \mathfrak{n}$. ▫

Satz 78 (Dedekindbereiche lokal charakterisiert)

Sei A ein noetherscher Integritätsbereich. Wir erinnern an die Definitionen 50*,* 52 *und* 73*.*

Es ist A dedekindsch genau dann, wenn $A_\mathfrak{p}$ ein diskreter Bewertungsring ist für alle $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$.

Beweis. O.E. ist A kein Körper. Schreibe $K := \mathrm{Quot}(A)$.

Ist A dedekindsch, dann ist auch $A_\mathfrak{p}$ ein diskreter Bewertungsring; cf. Bemerkung 74.

Sei umgekehrt $A_\mathfrak{p}$ ein diskreter Bewertungsring für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$.

Zeigen wir, daß A ganzabgeschlossen ist. Sei $x \in \Gamma_K(A)$. Dann ist $K \overset{\text{A. 11.(2)}}{=} \mathrm{Quot}(A_\mathfrak{p})$ und $x \in \Gamma_K(A_\mathfrak{p}) = A_\mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$, da $A_\mathfrak{p}$ als Hauptidealbereich ganzabgeschlossen ist; cf. Aufgabe 6.(1). Da A kein Körper ist, liegen alle maximalen Ideale von A in $\mathrm{Ideale}^\times_{\mathrm{prim}}(A)$. Folglich ist $x \in A_\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ von A. Also ist $x \in A$; cf. Lemma 77. Somit ist $A = \Gamma_K(A)$.

Zeigen wir, daß jedes $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ ein maximales Ideal ist. *Annahme,* nicht. Dann gibt es ein maximales Ideal $\mathfrak{q}$ mit $(0) \subset \mathfrak{p} \subset \mathfrak{q}$. Dann gibt es in $A_\mathfrak{q}$ die Kette $(0) \subset \mathfrak{p}_\mathfrak{q} \subset \mathfrak{q}_\mathfrak{q}$ von Primidealen; cf. Aufgabe 10.(2). Also ist $A_\mathfrak{p}$ nicht dedekindsch, insbesondere also kein Hauptidealbereich; cf. Bemerkung 53. Wir haben einen *Widerspruch.* ▫

Beispiel 79 Wir betrachten den Dedekindring $D := \mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$; cf. Aufgabe 3. Es ist darin

$$\mathfrak{p} \;:=\; (2, 1+\sqrt{-5})$$

ein Primideal, kein Hauptideal, und es ist $\mathfrak{p}^2 = (2)$; cf. Lösung zu Aufgabe 27.(3.i). Es ist $(1+\sqrt{-5}) \subseteq \mathfrak{p}$ und also $\mathrm{v}_\mathfrak{p}(1+\sqrt{-5}) \geqslant 1$; cf. Aufgabe 29.(4). Es ist $(1+\sqrt{-5}) \not\subseteq \mathfrak{p}^2$ und also $\mathrm{v}_\mathfrak{p}(1+\sqrt{-5}) < 2$; cf. Aufgabe 29.(5). Somit ist $\mathrm{v}_\mathfrak{p}(1+\sqrt{-5}) = 1$. Es folgt $\mathfrak{p}_\mathfrak{p} = (1+\sqrt{-5})_\mathfrak{p} \subseteq D_\mathfrak{p}$; cf. Aufgabe 29.(8).

Man kann auch direkt sehen, daß $\mathfrak{p}_\mathfrak{p} = (2, 1+\sqrt{-5})_\mathfrak{p} = (1+\sqrt{-5})_\mathfrak{p}$ ist: Es ist $\frac{2}{1+\sqrt{-5}} = \frac{1-\sqrt{-5}}{3} \in D_\mathfrak{p}$, da $3 \notin \mathfrak{p}$ ist, da sonst $3 - 2 = 1$ in $\mathfrak{p}$ läge.

Meist schreibt man wieder

$$\mathfrak{p}_\mathfrak{p} = (1+\sqrt{-5})\ ,$$

nur nun das Idealerzeugnis in $D_\mathfrak{p}$ gebildet.

2.3.2 Lokalisieren gebrochener Ideale

Sei D ein Dedekindbereich. Sei $K := \mathrm{Quot}(D)$. Sei $S \subseteq D^\times$ mit $1 \in S$ und $st \in S$ für $s, t \in D$ gegeben; cf. Aufgabe 10. Es ist $S^{-1}D$ ein Dedekindbereich; cf. Lemma 70.(6).

Definition 80 Sei $\mathfrak{g} \in \underline{\text{Ideale}}^\times(D)$. Sei $\mathfrak{g} = x\mathfrak{a}$ mit $x \in K^\times$ und $\mathfrak{a} \in \text{Ideale}^\times(D)$. Schreibe

$$S^{-1}\mathfrak{g} \;:=\; xS^{-1}\mathfrak{a} \;=\; \{\, y\,\frac{1}{s} \in K \;:\; y \in \mathfrak{g},\; s \in S\,\} \;\subseteq\; K\;,$$

wobei zweiterer Ausdruck die Unabhängigkeit von der Wahlen von x und von $\mathfrak{a}$ belegt.

Ist $\mathfrak{g} \in \text{Ideale}^\times(D)$, so stimmen die hier und die in Aufgabe 10.(1) gegebenen Definitionen von $S^{-1}\mathfrak{g}$ überein.

Ist $\mathfrak{p} \in \text{Ideale}^\times_{\text{prim}}(D)$ und ist $S = D \smallsetminus \mathfrak{p}$, so schreiben wir $\mathfrak{g}_\mathfrak{p} := S^{-1}\mathfrak{g}$.

Bemerkung 81 Seien $\mathfrak{g}$, $\mathfrak{h} \in \underline{\text{Ideale}}^\times(D)$ gegeben.

(1) Es ist $S^{-1}\mathfrak{g} \in \underline{\text{Ideale}}^\times(S^{-1}D)$. Cf. Aufgabe 33.(1).

(2) Es ist $S^{-1}(\mathfrak{g}\mathfrak{h}) = (S^{-1}\mathfrak{g})(S^{-1}\mathfrak{h})$ und $(S^{-1}\mathfrak{g})^{-1} = S^{-1}(\mathfrak{g}^{-1})$. Cf. Aufgabe 33.(2).

(3) Es ist $S^{-1}(\mathfrak{g}+\mathfrak{h}) = S^{-1}\mathfrak{g}+S^{-1}\mathfrak{h}$ und $S^{-1}(\mathfrak{g}\cap\mathfrak{h}) = S^{-1}\mathfrak{g}\cap S^{-1}\mathfrak{h}$. Cf. Aufgabe 33.(3).

(4) Sei $\mathfrak{p} \in \text{Ideale}^\times_{\text{prim}}(D)$. Es ist $\mathfrak{g}_\mathfrak{p} = (\mathfrak{p}_\mathfrak{p})^{\text{v}_\mathfrak{p}(\mathfrak{g})}$. Cf. Aufgabe 33.(4).

(5) Es ist $\mathfrak{g} = \bigcap_{\mathfrak{p}\in\text{Ideale}^\times_{\text{prim}}(D)} \mathfrak{g}_\mathfrak{p}$. Cf. Aufgabe 33.(5).

2.3.3 Die Idealnorm

Sei A ein Dedekindbereich. Sei $K := \text{Quot}(A)$ perfekt. Sei $L|K$ eine endliche Körpererweiterung. Schreibe $\ell := [L : K]$.

Sei $B := \Gamma_L(A)$. Es ist B ein Dedekindbereich; cf. Lemma 54.

Bemerkung 82 *Sei* $\mathfrak{p} \in \text{Ideale}^\times_{\text{prim}}(A)$. *Schreibe* $S := A \smallsetminus \mathfrak{p}$.

Schreibe $\mathfrak{g}_\mathfrak{p} := S^{-1}\mathfrak{g}$ *für* $\mathfrak{g} \in \underline{\text{Ideale}}^\times(B)$ *; cf. Aufgabe* 10.(1).

Insbesondere ist $B_\mathfrak{p} = S^{-1}B$.

Es sind $A \subseteq A_\mathfrak{p} \subseteq K$ *und* $B \subseteq B_\mathfrak{p} \subseteq L$ *Inklusionen von Teilringen; cf. Aufgabe* 10.(1).

Zerlege

$$\mathfrak{p}B \;=\; \prod_{i\in[1,n]} \mathfrak{q}_i^{\gamma_i}$$

mit $n \geqslant 0$, $\mathfrak{q}_i \in \text{Ideale}^\times_{\text{prim}}(B)$ *und* $\gamma_i \geqslant 1$ *für* $i \in [1,n]$ *; cf. Satz* 63.(1).

(1) *Es ist* $\text{Quot}(B) = \text{Quot}(B_\mathfrak{p}) = L$.

(2) *Es ist* $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$.

(3) *Es ist $A_\mathfrak{p}$ ein diskreter Bewertungsring und $B_\mathfrak{p}$ ein Hauptidealbereich.*

(4) *Es ist* $\mathrm{Ideale}^\times_{\mathrm{prim}}(B_\mathfrak{p}) = \{\, (\mathfrak{q}_i)_\mathfrak{p} \,:\, i \in [1,n] \,\}$.

Beweis.

Ad (1). Mit $S_0 := A^\times$ folgt $S_0^{-1}B = S_0^{-1}\Gamma_L(A) = \Gamma_L(S_0^{-1}A) = \Gamma_L(K) = L$; cf. Lemma 70.(4). Cf. also Lemma 27. Da $S_0^{-1}B \subseteq \mathrm{Quot}(B) \subseteq L$, folgt $\mathrm{Quot}(B) = L$. Dann ist (nach Identifikation) auch $\mathrm{Quot}(B_\mathfrak{p}) = L$; cf. Aufgabe 11.(2).

Ad (2). Es ist

$$B_\mathfrak{p} \;=\; S^{-1}\Gamma_L(A) \;\overset{\text{L. 70.(4)}}{=}\; \Gamma_L(S^{-1}A) \;=\; \Gamma_L(A_\mathfrak{p})\;.$$

Ad (3, 4). Da nach Satz 78 nun $A_\mathfrak{p}$ ein diskreter Bewertungsring, insbesondere also ein Hauptidealbereich und somit ein Dedekindbereich ist, ist mithin auch $B_\mathfrak{p}$ ein Dedekindbereich; cf. Bemerkung 53, Lemma 54. Es ist

$$\begin{aligned}\mathrm{Ideale}_{\mathrm{prim}}(B_\mathfrak{p}) &= \{\, \mathfrak{q}_\mathfrak{p} \,:\, \mathfrak{q} \in \mathrm{Ideale}_{\mathrm{prim}}(B),\ \mathfrak{q} \cap S = \emptyset \,\} \\ &= \{\, \mathfrak{q}_\mathfrak{p} \,:\, \mathfrak{q} \in \mathrm{Ideale}_{\mathrm{prim}}(B),\ \mathfrak{q} \cap A \subseteq \mathfrak{p} \,\}\;,\end{aligned}$$

cf. Aufgabe 10.(1). Für $\mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(B_\mathfrak{p})$ ist $\mathfrak{q} \cap A \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$; cf. Lemma 54. Da A dedekindsch ist, besteht $\mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ aus maximalen Idealen, und somit ist

$$\mathrm{Ideale}^\times_{\mathrm{prim}}(B_\mathfrak{p}) \;=\; \{\, \mathfrak{q}_\mathfrak{p} \,:\, \mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(B),\ \mathfrak{q} \cap A = \mathfrak{p} \,\}\;.$$

Für $\mathfrak{q} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(B)$ ist $\mathfrak{q} \cap A = \mathfrak{p}$ genau dann, wenn $\mathfrak{p} \subseteq \mathfrak{q} \cap A$, i.e. wenn $\mathfrak{p}B \subseteq \mathfrak{q}$ liegt. Nach Aufgabe 29.(1) ist das genau dann der Fall, wenn $\mathfrak{q} \in \{\, \mathfrak{q}_i \,:\, i \in [1,n] \,\}$ ist. Somit ist $\mathrm{Ideale}^\times_{\mathrm{prim}}(B_\mathfrak{p}) = \{\, (\mathfrak{q}_i)_\mathfrak{p} \,:\, i \in [1,n] \,\}$ und damit (4) gezeigt. Als Dedekindbereich mit endlich vielen maximalen Idealen ist nun $B_\mathfrak{p}$ ein Hauptidealbereich; cf. Lemma 72. Dies zeigt vollends (3). ▫

Definition 83 Ist X eine Menge und $f : X \longrightarrow K$ eine Abbildung, so schreiben wir auch

$$\begin{aligned}(\, f(x) \,:\, x \in X \,) \;&:=\; {}_A\langle\, f(x) \,:\, x \in X \,\rangle \\ &=\; \{\, \textstyle\sum_{i\in[1,k]} a_i f(x_i) \,:\, k \geqslant 0,\ a_i \in A \text{ und } x_i \in X \text{ für } i \in [1,k] \,\} \;\subseteq\; K\end{aligned}$$

für das A-lineare Erzeugnis von $f(X)$ in K.

Definition 84 Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$. Sei die *(gebrochene) Idealnorm* von $\mathfrak{g}$ definiert durch

$$\mathrm{N}_{L|K}(\mathfrak{g}) \;:=\; (\, \mathrm{N}_{L|K}(g) \,:\, g \in \mathfrak{g} \,) \;\subseteq\; K\;.$$

Also Vorsicht, wenn $\mathrm{N}_{L|K}$ auf ein Ideal oder ein gebrochenes Ideal angewandt wird, so ist dies nicht lediglich als elementweise Anwendung von $\mathrm{N}_{L|K}$ zu verstehen – vielmehr muß nach elementweiser Anwendung von $\mathrm{N}_{L|K}$ noch das A-lineare Erzeugnis gebildet werden. Cf. Aufgabe 35.(10).

Bemerkung 85 *Sei* $\mathfrak{g} \in \underline{\text{Ideale}}^{\times}(B)$.

Es gibt ein $t \in A^{\times}$ *und ein* $\mathfrak{b} \in \text{Ideale}^{\times}(B)$ *mit* $\mathfrak{g} = \frac{1}{t}\mathfrak{b}$.

Beweis. Schreibe $\mathfrak{g} = x\mathfrak{b}_0$ mit $x \in L^{\times}$ und $\mathfrak{b}_0 \in \text{Ideale}^{\times}(B)$. Wähle ein $t \in A^{\times}$ mit $tx \in B^{\times}$; cf. Lemma 27. Mit $\mathfrak{b} := tx\mathfrak{b}_0 \in \text{Ideale}^{\times}(B)$ ist dann $\mathfrak{g} = \frac{1}{t}\mathfrak{b}$. ▫

Bemerkung 86

(1) *Für* $\mathfrak{g} \in \underline{\text{Ideale}}^{\times}(B)$ *ist* $\text{N}_{L|K}(\mathfrak{g}) \in \underline{\text{Ideale}}^{\times}(A)$.

(2) *Für* $\mathfrak{b} \in \text{Ideale}^{\times}(B)$ *ist* $\text{N}_{L|K}(\mathfrak{b}) \in \text{Ideale}^{\times}(A)$.

(3) *Für* $y \in L^{\times}$ *ist* $\text{N}_{L|K}(\,(y)\,) = (\,\text{N}_{L|K}(y)\,)$.

Beweis.

Ad (2). Folgt nach Konstruktion.

Ad (1). Schreibe $\mathfrak{g} = \frac{1}{t}\mathfrak{b}$ mit $t \in A^{\times}$ und $\mathfrak{b} \in \text{Ideale}^{\times}(B)$; cf. Bemerkung 85.

Es wird $\text{N}_{L|K}(\mathfrak{g}) = (\,\text{N}_{L|K}(\frac{1}{t}b) \,:\, b \in \mathfrak{b}\,) = \frac{1}{t^{\ell}}(\,\text{N}_{L|K}(b) \,:\, b \in \mathfrak{b}\,) = \frac{1}{t^{\ell}}\,\text{N}_{L|K}(\mathfrak{b})$. Nach Konstruktion ist $\text{N}_{L|K}(\mathfrak{b})$ ein Ideal in B. Da $\mathfrak{b} \neq 0$, ist $\text{N}_{L|K}(\mathfrak{b}) \neq 0$; cf. Definition 12. Also ist $\text{N}_{L|K}(\mathfrak{g})$ ein gebrochenes Ideal von A.

Ad (3). Zu $\overset{!}{\supseteq}$. Es ist $\text{N}_{L|K}(y) \in \text{N}_{L|K}(\,(y)\,)$.

Zu $\overset{!}{\subseteq}$. Für $b \in B$ ist $\text{N}_{L|K}(by) = \text{N}_{L|K}(b)\,\text{N}_{L|K}(y) \in (\,\text{N}_{L|K}(y)\,)$. ▫

Lemma 87 *Sei* $\mathfrak{p} \in \text{Ideale}^{\times}_{\text{prim}}(A)$. *Sei* $\mathfrak{g} \in \underline{\text{Ideale}}^{\times}(B)$.

Es ist $\text{N}_{L|K}(\mathfrak{g})_{\mathfrak{p}} = \text{N}_{L|K}(\mathfrak{g}_{\mathfrak{p}})$ *als gebrochene Ideale von* $A_{\mathfrak{p}}$.

Beweis.

Ad $\overset{!}{\subseteq}$. Es ist $\text{N}_{L|K}(\mathfrak{g}) \subseteq \text{N}_{L|K}(\mathfrak{g}_{\mathfrak{p}})$, und letzteres ist ein gebrochenes Ideal von $A_{\mathfrak{p}}$.

Ad $\overset{!}{\supseteq}$. Für $s \in A \smallsetminus \mathfrak{p}$ und $g \in \mathfrak{g}$ wird $\text{N}_{L|K}(\frac{g}{s}) = \frac{1}{s^{\ell}}\,\text{N}_{L|K}(g) \in \text{N}_{L|K}(\mathfrak{g})_{\mathfrak{p}}$. ▫

Lemma 88 *Seien* $\mathfrak{g}$, $\tilde{\mathfrak{g}} \in \underline{\text{Ideale}}^{\times}(B)$.

Es ist $\text{N}_{L|K}(\mathfrak{g} \cdot \tilde{\mathfrak{g}}) = \text{N}_{L|K}(\mathfrak{g}) \cdot \text{N}_{L|K}(\tilde{\mathfrak{g}})$.

> Versucht man, direkt nach Definition 84 vorzugehen, so kann man die Inklusion $\supseteq$ erkennen. Die Inklusion $\subseteq$ scheint mehr Probleme zu bereiten, da $\text{N}_{L|K}(g_1\tilde{g}_1 + \cdots + g_k\tilde{g}_k)$ nicht ohne weiteres als A-Linearkombination von Elementen der Form $\text{N}_{L|K}(g)\,\text{N}_{L|K}(\tilde{g}) = \text{N}_{L|K}(g\tilde{g})$ geschrieben werden kann, da sich Norm und Summe nicht gut vertragen. Hierbei war $k \geqslant 0$, $g_i \in \mathfrak{g}$ und $\tilde{g}_i \in \tilde{\mathfrak{g}}$ für $i \in [1, k]$, sowie $g \in \mathfrak{g}$ und $\tilde{g} \in \tilde{\mathfrak{g}}$.

Beweis. Wir schreiben kurz $\mathrm{N} := \mathrm{N}_{L|K}$.

Es genügt, $\mathrm{N}(\mathfrak{g}\tilde{\mathfrak{g}})_{\mathfrak{p}} \stackrel{!}{=} (\mathrm{N}(\mathfrak{g})\,\mathrm{N}(\tilde{\mathfrak{g}}))_{\mathfrak{p}}$ für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$ zu zeigen; cf. Bemerkung 81.(5).

Dank Lemma 87 und Bemerkung 81.(2) bedeutet dies $\mathrm{N}(\mathfrak{g}_{\mathfrak{p}}\tilde{\mathfrak{g}}_{\mathfrak{p}}) \stackrel{!}{=} \mathrm{N}(\mathfrak{g}_{\mathfrak{p}})\,\mathrm{N}(\tilde{\mathfrak{g}}_{\mathfrak{p}})$.

Nun sind $A_{\mathfrak{p}}$ und $B_{\mathfrak{p}}$ Hauptidealbereiche, es ist $K = \mathrm{Quot}(A_{\mathfrak{p}})$ sowie $L = \mathrm{Quot}(B_{\mathfrak{p}})$, und es ist $B_{\mathfrak{p}} = \Gamma_L(A_{\mathfrak{p}})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Ist nun $\mathfrak{g} = (g)$ und $\tilde{\mathfrak{g}} = (\tilde{g})$ mit $g, \tilde{g} \in L^{\times}$, dann wird in der Tat

$$\begin{aligned} \mathrm{N}(\mathfrak{g}\tilde{\mathfrak{g}}) \;&=\; \mathrm{N}(\,(g\tilde{g})\,) \;\stackrel{\text{B. 86.(3)}}{=}\; (\,\mathrm{N}(g\tilde{g})\,) \;=\; (\,\mathrm{N}(g)\,\mathrm{N}(\tilde{g})\,) \\ &=\; (\,\mathrm{N}(g)\,)(\,\mathrm{N}(\tilde{g})\,) \;\stackrel{\text{B. 86.(3)}}{=}\; \mathrm{N}(\,(g)\,)\,\mathrm{N}(\,(\tilde{g})\,) \;=\; \mathrm{N}(\mathfrak{g})\,\mathrm{N}(\tilde{\mathfrak{g}})\;. \end{aligned}$$

□

Bemerkung 89 $\mathfrak{h} \in \underline{\mathrm{Ideale}}^{\times}(B)$.

Jede A-lineare Basis von $\mathfrak{h}$ ist auch eine K-lineare Basis von L.

Falls A ein Hauptidealbereich ist, dann existiert eine A-lineare Basis von $\mathfrak{h}$.

Beweis. Wähle $z \in \mathfrak{h}^{\times}$. Es ist $(z) = Bz \subseteq \mathfrak{h}$.

Sei $\underline{h}$ eine A-lineare Basis von $\mathfrak{h}$. Da $\underline{h}$ ein A-linear unabhängiges Tupel ist, ist es auch K-linear unabhängig. Bleibt zu zeigen, daß ${}_K\langle\underline{h}\rangle = L$ ist. Sei $y \in L$ gegeben. Schreibe $yz^{-1} = a^{-1}b$ für ein $a \in A^{\times}$ und ein $b \in B$; cf. Lemma 27. Dann ist $bz \in \mathfrak{h} = {}_A\langle\underline{h}\rangle \subseteq {}_K\langle\underline{h}\rangle$ und also auch $y = a^{-1}bz \in {}_K\langle\underline{h}\rangle$.

Sei nun A ein Hauptidealbereich. Schreibe $\mathfrak{h} = x\mathfrak{b}$ für $x \in L^{\times}$ und $\mathfrak{b} \in \mathrm{Ideale}^{\times}(B)$ geeignet. Es wird

$$(z) \;\subseteq\; \mathfrak{h} \;=\; x\mathfrak{b} \;\subseteq\; xB \;=\; (x)\;,$$

und als A-Moduln ist $B \simeq (z)$ und $B \simeq (x)$. Dank Lemma 33 sind also (z) und (x) endlich erzeugt freie A-Moduln von Rang ℓ. Dank Aufgabe 13.(2) ist nun auch $\mathfrak{h}$ ein endlich erzeugt freier A-Modul von Rang ℓ. □

> Cf. Lemma 33. Im zweiten Argument wird $(z) \subseteq \mathfrak{h}$ nur gebraucht, um den Rang des A-Moduls $\mathfrak{h}$ zu ℓ zu bestimmen, welcher auch daraus folgt, daß eine A-lineare Basis von $\mathfrak{h}$ auch eine K-lineare Basis von L ist.

Lemma 90 *Sei* $\mathfrak{h} \in \underline{\mathrm{Ideale}}^{\times}(B)$.

Existiere eine A-lineare Basis $\underline{g} = (\,g_i \;:\; i \in [1,\ell]\,)$ von B und eine A-lineare Basis $\underline{h} = (\,h_j \;:\; j \in [1,\ell]\,)$ von $\mathfrak{h}$.

Sei $h_j =: \sum_{i\in[1,\ell]} s_{i,j}\,g_i$ für $j \in [1,\ell]$, mit $S := (s_{i,j})_{i,j} \in K^{\ell\times\ell}$.

Es ist $\mathrm{N}_{L|K}(\mathfrak{h}) = (\,\det(S)\,)$.

Beweis. Es genügt $\mathrm{N}_{L|K}(\mathfrak{h})_{\mathfrak{p}} \stackrel{!}{=} (\det(S))_{\mathfrak{p}}$ zu zeigen für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$; cf. Bemerkung 81.(5). I.e. wir haben $\mathrm{N}_{L|K}(\mathfrak{h}_{\mathfrak{p}}) \stackrel{!}{=} (\det(S))$ zu zeigen, letzteres gelesen als gebrochenes Hauptideal von $A_{\mathfrak{p}}$; cf. Lemma 87. Da $\mathrm{Quot}(B_{\mathfrak{p}}) = L$ und da $B_{\mathfrak{p}} = \Gamma_L(A_{\mathfrak{p}})$ ist nach Bemerkung 82.(1, 2), und da $\underline{g}$ auch eine $A_{\mathfrak{p}}$-lineare Basis von $B_{\mathfrak{p}}$ sowie $\underline{h}$ auch eine $A_{\mathfrak{p}}$-lineare Basis von $\mathfrak{h}_{\mathfrak{p}}$ ist, genügt es, die Behauptung für $A_{\mathfrak{p}}$ statt für A zu zeigen. Es ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring und $B_{\mathfrak{p}}$ ein Hauptidealbereich; cf. Bemerkung 82.(3).

Somit dürfen wir annehmen, daß A ein diskreter Bewertungsring, B ein Hauptidealbereich und $\mathfrak{h} \in \underline{\mathrm{Ideale}}^{\times}(B)$ ist. Schreibe $\mathfrak{h} = (z)$ für ein geeignetes $z \in L^{\times}$. Es ist $\mathrm{N}_{L|K}(\mathfrak{h}) = \mathrm{N}_{L|K}((z)) \stackrel{\text{B. 86.(3)}}{=} (\mathrm{N}_{L|K}(z))$. Betrachte die K-lineare Abbildung $\lambda_z : L \longrightarrow L$, $y \longmapsto zy$. Bezüglich der A-linearen Basis $(z^{-1}h_j \ : \ j \in [1,\ell])$ von $z^{-1}\mathfrak{h} = z^{-1}(z) = (1) = B$ und bezüglich der A-linearen Basis $\underline{g}$ von B wird λ_z von der Matrix S beschrieben, da $z(z^{-1}h_j) = \sum_{i\in[1,\ell]} s_{i,j}\, g_i$ für $j \in [1,\ell]$.

Sei $g_k =: \sum_{j\in[1,\ell]} u_{j,k}\, z^{-1}h_j$ für $k \in [1,\ell]$, mit $u_{j,k} \in A$ stets. Sei $z^{-1}h_j =: \sum_{k\in[1,\ell]} v_{k,j}\, g_k$ für $j \in [1,\ell]$, mit $v_{k,j} \in A$ stets. Mit $U := (u_{j,k})_{j,k} \in A^{\ell\times\ell}$ und $V := (v_{k,j})_{k,j} \in A^{\ell\times\ell}$ folgt dann

$$\sum_{i\,\in\,[1,\ell]} \partial_{i,k}\, g_i \;=\; g_k \;=\; \sum_{j,\,i\,\in\,[1,\ell]} u_{j,k}\, v_{i,j}\, g_i$$

für $k \in [1,\ell]$, also $\sum_{j\in[1,\ell]} v_{i,j}u_{j,k} = \partial_{i,k}$ stets, also $VU = \mathrm{E}_{\ell}$, also $\det(U) \in \mathrm{U}(A)$, also $U \in \mathrm{GL}_{\ell}(A)$.

Sei ferner $zg_k = \sum_{i\in[1,\ell]} t_{i,k}\, g_i$ für $i \in [1,\ell]$, mit $t_{i,k} \in K$ stets. Schreibe $T := (t_{i,k})_{i,k} \in K^{\ell\times\ell}$. Es ist $\det(T) = \mathrm{N}_{L|K}(z)$; cf. Definition 12.

Dann ist $zg_k = \sum_{j\in[1,\ell]} u_{j,k}\, h_j \;=\; \sum_{i,\,j\,\in\,[1,\ell]} u_{j,k}\, s_{i,j}\, g_i$ stets, folglich $\sum_{j\in[1,\ell]} u_{j,k}\, s_{i,j} = t_{i,k}$ stets, i.e. $SU = T$.

Insgesamt folgt

$$\mathrm{N}_{L|K}(\mathfrak{h}) \;=\; (\mathrm{N}_{L|K}(z)) \;=\; (\det(T)) \;=\; (\det(S)\det(U)) \;=\; (\det(S))\,.$$

□

Lemma 91 *Sei $F|\mathbf{Q}$ eine endliche Körpererweiterung. Sei $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathcal{O}_F)$.*

Es ist $\mathrm{N}_{F|\mathbf{Q}}(\mathfrak{a}) = (|\mathcal{O}_F/\mathfrak{a}|)$ als Ideale in $\mathbf{Z}$.

Beweis. Schreibe $f := [F : \mathbf{Q}]$. Es gibt eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_F$; cf. Lemma 33.

Es ist $\mathfrak{a}$ ein endlich erzeugt freier $\mathbf{Z}$-Modul mit $\mathrm{rk}_{\mathbf{Z}}\,\mathfrak{a} = f$.

Beschreibe $S \in \mathbf{Z}^{f\times f}$ die Einbettungsabbildung von $\mathfrak{a}$ nach $\mathcal{O}_F$ bezüglich jeweils gewählter $\mathbf{Z}$-linearer Basen.

Es ist $|\mathcal{O}_F/\mathfrak{a}| = |\det(S)|$; cf. Aufgabe 14.(2).

Auf der anderen Seite ist $\mathrm{N}_{F|\mathbf{Q}}(\mathfrak{a}) = (\det(S)) = (|\det(S)|)$; cf. Lemma 90.

Insgesamt ist $\mathrm{N}_{F|\mathbf{Q}}(\mathfrak{a}) = (|\mathcal{O}_F/\mathfrak{a}|)$. □

Bemerkung 92 *Sei $F|\mathbf{Q}$ eine endliche Körpererweiterung. Seien $\mathfrak{a}$, $\mathfrak{b} \in \mathrm{Ideale}^\times(\mathcal{O}_F)$. Es ist $|\mathcal{O}_K/\mathfrak{a}| \cdot |\mathcal{O}_K/\mathfrak{b}| = |\mathcal{O}_K/(\mathfrak{a}\mathfrak{b})|$.*

Beweis. Es ist

$$\begin{array}{rcl}(|\mathcal{O}_F/\mathfrak{a}| \cdot |\mathcal{O}_F/\mathfrak{b}|) & = & (|\mathcal{O}_F/\mathfrak{a}|)(|\mathcal{O}_F/\mathfrak{b}|) \\ & \overset{\text{L. 91}}{=} & \mathrm{N}_{F|\mathbf{Q}}(\mathfrak{a})\,\mathrm{N}_{F|\mathbf{Q}}(\mathfrak{b}) \\ & \overset{\text{L. 88}}{=} & \mathrm{N}_{F|\mathbf{Q}}(\mathfrak{a}\mathfrak{b}) \\ & \overset{\text{L. 91}}{=} & (|\mathcal{O}_F/(\mathfrak{a}\mathfrak{b})|)\end{array}$$

als Ideale in $\mathbf{Z}$. Folglich ist auch $|\mathcal{O}_K/\mathfrak{a}| \cdot |\mathcal{O}_K/\mathfrak{b}| = |\mathcal{O}_K/(\mathfrak{a}\mathfrak{b})|$. ▫

Beispiel 93 Es ist $\mathfrak{p} := (2, 1+\sqrt{-5})$ kein Hauptideal in $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$. Denn es ist $\mathfrak{p} = \mathbf{Z}\langle 2, 2\sqrt{-5}, 1+\sqrt{-5}, -5+\sqrt{-5}\rangle = \mathbf{Z}\langle 2, 1+\sqrt{-5}\rangle$, hat also

$$\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(\mathfrak{p}) \;=\; (|\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}|) \;\overset{\text{A. 14.(2)}}{=}\; (\det \left(\begin{smallmatrix}2&1\\0&1\end{smallmatrix}\right)) \;=\; (2)\,,$$

wohingegen für ein Hauptideal erzeugt von $a + b\sqrt{-5}$ mit a, $b \in \mathbf{Z}$

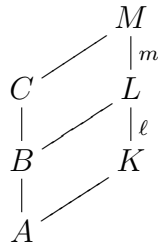
$$\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(\,(a+b\sqrt{-5})\,) \;=\; (\,\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(a+b\sqrt{-5})\,) \;=\; (a^2+5b^2)$$

wird, was nicht dasselbe sein kann.

Das, leicht verkleidet, war auch die Lösung zu Aufgabe 27.(1).

2.3.4 Differente und Diskriminantenideal

Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt. Seien $M|L|K$ endliche Körpererweiterungen. Schreibe $m := [M : L]$ und $\ell := [L : K]$. Seien $B := \Gamma_L(A)$ und $C := \Gamma_M(A)$.



Wir erinnern an $B^{\#,A} = \{\, y \in L \,:\, \mathrm{Tr}_{L|K}(yB) \subseteq A \,\}$; cf. Definition 29.

Bemerkung 94

(1) *Es ist $B^{\#,A} \in \underline{\mathrm{Ideale}}^\times(B)$.*

(2) *Es ist* $(B^{\#,A})^{-1} \in \mathrm{Ideale}^{\times}(B)$.

(3) *Es ist* $B^{\#,A}$ *terminal in* $\{\, \mathfrak{g} \in \underline{\mathrm{Ideale}}^{\times}(B) \,:\, \mathrm{Tr}_{L|K}(\mathfrak{g}) \subseteq A \,\}$.
Für $\mathfrak{g} \in \underline{\mathrm{Ideale}}^{\times}(B)$ *ist also genau dann* $\mathfrak{g} \subseteq B^{\#,A}$, *wenn* $\mathrm{Tr}_{L|K}(\mathfrak{g}) \subseteq A$ *ist.*

Beweis. Kürze $B^{\#} = B^{\#,A}$ ab.

Ad (1). Sei $\underline{y} = (\, y_i \,:\, i \in [1,\ell]\,)$ eine K-lineare Basis von L, deren Elemente in B liegen; cf. Lemma 28. Sei $Y := {}_A\langle \underline{y} \rangle$.

Sei $\underline{y'} = (\, y'_i \,:\, i \in [1,\ell]\,)$ die zu $\underline{y}$ bezüglich Spurbilinearform duale Basis; cf. Lemma 22. Dann ist $Y^{\#} = {}_A\langle \underline{y'} \rangle$; cf. Lemma 31.(3). Es ist $Y \subseteq B \subseteq B^{\#} \subseteq Y^{\#}$; cf. Lemma 31.(2), Bemerkung 30. Sei $s \in A^{\times}$ so gewählt, daß $sy'_i \in B$ liegt für $i \in [1,\ell]$; cf. Lemma 27. Dann ist $B^{\#} = \frac{1}{s}(sB^{\#})$ mit $sB^{\#} \subseteq B$.

Bleibt zu zeigen, daß $sB^{\#}$ ein Ideal von B ist. Es ist $0 \in sB^{\#}$.

Seien $z,\, z' \in B^{\#}$ und $b,\, b' \in B$. Zu zeigen ist $b(sz) + b'(sz') \overset{!}{\in} sB^{\#}$, i.e. $bz + b'z' \overset{!}{\in} B^{\#}$.
Sei $\tilde{b} \in B$. Zu zeigen ist $\mathrm{Tr}_{L|K}((bz + b'z')\tilde{b}) \overset{!}{\in} A$. In der Tat ist $\mathrm{Tr}_{L|K}((bz + b'z')\tilde{b}) = \mathrm{Tr}_{L|K}(z(b\tilde{b})) + \mathrm{Tr}_{L|K}(z'(b'\tilde{b})) \in A$.

Ad (2). Es folgt aus $(1) = B \subseteq B^{\#}$, daß $B = (1) = (1)^{-1} \supseteq (B^{\#})^{-1}$ ist.

Ad (3). Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^{\times}(B)$ gegeben.

Ist $\mathfrak{g} \subseteq B^{\#}$, dann ist $\mathrm{Tr}_{L|K}(\mathfrak{g}) \subseteq \mathrm{Tr}_{L|K}(B^{\#}) = \mathrm{Tr}_{L|K}(B^{\#} \cdot 1) \subseteq A$.

Sei umgekehrt $\mathrm{Tr}_{L|K}(\mathfrak{g}) \subseteq A$. Für $g \in \mathfrak{g}$ ist $gB \subseteq \mathfrak{g}$, also $\mathrm{Tr}_{L|K}(gB) \subseteq \mathrm{Tr}_{L|K}(\mathfrak{g}) \subseteq A$, mithin $g \in B^{\#}$. Insgesamt ist also $\mathfrak{g} \subseteq B^{\#}$. ▫

Definition 95

(1) Sei
$$\mathfrak{D}_{L|K,A} \;:=\; (B^{\#,A})^{-1} \;\in\; \mathrm{Ideale}^{\times}(B)$$
die *Differente* von $L|K$ bezüglich A.

(2) Sei
$$\mathfrak{d}_{L|K,A} \;:=\; \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A}) \;\in\; \mathrm{Ideale}^{\times}(A)$$
das *Diskriminantenideal* von $L|K$ bezüglich A; cf. Definition 84, Bemerkung 86.(2).

Lemma 96 *Existiere eine* A*-lineare Basis* $\underline{g} = (\, g_i \,:\, i \in [1,\ell]\,)$ *von* B.
Dann ist $\mathfrak{d}_{L|K,A} = (\Delta_{L|K,\underline{g}})$.

Beweis. Sei $\underline{g'} = (\, g'_j \,:\, j \in [1,\ell]\,)$ die zu $\underline{g}$ bezüglich Spurbilinearform duale Basis. Dann ist $\underline{g'}$ eine A-lineare Basis von $B^{\#,A}$; cf. Lemma 31.(3). Wir haben $\mathrm{Gram}_{L|K,\underline{g}} =$

$(\mathrm{Tr}_{L|K}(g_j g_i))_{j,i} \in A^{\ell\times\ell}$; cf. Lemmata 22 und 20.(2). Es ist

$$g_i \;=\; \sum_{j\in[1,\ell]} \mathrm{Tr}_{L|K}(g_j g_i) g'_j$$

für $i \in [1,\ell]$, da die Spurbilinearform nach Lemma 22 nichtausgeartet ist und da für $k \in [1,\ell]$ sich

$$\mathrm{Tr}_{L|K}(g_k(\sum_{j\in[1,\ell]} \mathrm{Tr}_{L|K}(g_j g_i) g'_j)) \;=\; \sum_{j\in[1,\ell]} \mathrm{Tr}_{L|K}(g_j g_i)\partial_{k,\,j} \;=\; \mathrm{Tr}_{L|K}(g_k g_i)$$

ergibt. Schreiben wir $\mathrm{Gram}^{-1}_{L|K,\,\underline{g}} =: (s_{i,\,j})_{i,\,j} \in K^{\ell\times\ell}$, so wird

$$g'_j \;=\; \sum_{k\in[1,\ell]} \partial_{j,k}\, g'_k = \sum_{i,\,k\,\in[1,\ell]} s_{i,\,j}\, \mathrm{Tr}_{L|K}(g_k g_i) g'_k \;=\; \sum_{i\in[1,\ell]} s_{i,\,j}\, g_i$$

für $j \in [1,\ell]$. Somit wird

$$\mathfrak{d}^{-1}_{L|K,A} \overset{\text{A. 34.(1)}}{=} \mathrm{N}_{L|K}(\mathfrak{D}^{-1}_{L|K,A}) \overset{\text{D. 95.(1)}}{=} \mathrm{N}_{L|K}(B^{\#,A}) \overset{\text{L. 90}}{=} (\,\det(\mathrm{Gram}^{-1}_{L|K,\,\underline{g}})\,)\,,$$

und daher

$$\mathfrak{d}_{L|K,A} \;=\; (\,\det(\mathrm{Gram}_{L|K,\,\underline{g}})\,) \overset{\text{L. 36}}{=} (\,\Delta_{L|K,\,\underline{g}}\,)\,.$$

□

Lemma 97 *Gebe es ein $b \in B$ mit $B = A[b]$. Dann ist $\mathfrak{D}_{L|K,A} = (\mu'_{b,K}(b)) \subseteq B$.*

Beweis. Es ist $L = K(b)$; cf. Lemma 27. Schreibe $\mu_{b,K}(X) =: \mu(X) =: \sum_{i\in[0,\ell]} a_i X^i$, wobei $a_i \in A$ stets und $a_\ell = 1$.

Schreibe $g(X) := \frac{\mu(X)}{X-b} = \sum_{i\in[0,\ell-1]} c_i X^i$, wobei $c_i \in B$ stets und $c_{\ell-1} = 1$.

Betrachte die A-lineare Basis

$$(\,b^i \;:\; i \in [0,\ell-1]\,)$$

von B.

Wir *behaupten*, daß die dazu bezüglich Spurbilinearform duale Basis gegeben ist durch

$$(\,\frac{c_i}{\mu'(b)} \;:\; i \in [0,\ell-1]\,)\,.$$

I.e. wir behaupten

$$\mathrm{Tr}_{L|K}(b^i \frac{c_j}{\mu'(b)}) \;\overset{!}{=}\; \partial_{i,\,j}$$

für $i,\, j \,\in\, [0,\ell-1]$.

Sei E Zerfällungskörper von $L|K$. Sei $G := \mathrm{Gal}(E|K) \geqslant \mathrm{Gal}(E|L) =: U$.

Sei $G = \bigsqcup_{k\in[1,\ell]} \sigma_k U$ mit $\sigma_k \in G$. Sei o.E. $\sigma_1 = \mathrm{id}_E$. Dann ist $\mu(X) = \prod_{k\in[1,\ell]}(X - \sigma_k(b))$; cf. Lemma 14. Hierbei ist $\sigma_k(b) \neq \sigma_{\tilde{k}}(b)$ für k, $\tilde{k} \in [1,\ell]$ mit $k \neq \tilde{k}$.

Wir setzen die K-lineare Abbildung $\mathrm{Tr}_{L|K} : L \longrightarrow K$ koeffizientenweise fort zu einer K-linearen Abbildung $\hat{\mathrm{Tr}}_{L|K} : L[X] \longrightarrow K[X]$, $\sum_{i\geqslant 0} u_i X^i \longmapsto \sum_i \mathrm{Tr}_{L|K}(u_i)X^i$.

Für $j \in [0,\ell-1]$ setzen wir den Körperautomorphismus $\sigma_j : E \longrightarrow E$ fort zu einem Ringautomorphismus $\hat{\sigma}_j : E[X] \longrightarrow E[X]$, $u(X) = \sum_{i\geqslant 0} u_i X^i \longmapsto \sum_i \sigma_j(u_i)X^i = u^{\sigma_j}(X)$; cf. [**5,** §1.6.2]. Für $u(X) \in L[X]$ ist also $\hat{\mathrm{Tr}}_{L|K}(u(X)) = \sum_{k\in[1,\ell]} u^{\sigma_k}(X)$.

Es ist

$$\mu(X) \;=\; g(X)(X-b)\;,$$

nach Produktregel also

$$\mu'(X) \;=\; g(X) + g'(X)(X-b)\;,$$

und somit

$$\mu'(b) \;=\; g(b)\;.$$

Sei $r \in [0,\ell-1]$. Für $k \in [1,\ell]$ ist

$$\hat{\sigma}_k\Big(g(X)\frac{b^r}{\mu'(b)}\Big) \;=\; g^{\sigma_k}(X)\frac{\sigma_k(b)^r}{\mu'(\sigma_k(b))}\quad,$$

und dieses Polynom wird beim Einsetzen von $\sigma_k(b)$ gleich $\sigma_k(b)^r$, beim Einsetzen von $\sigma_j(b)$ für $j \in [1,\ell] \smallsetminus \{k\}$ jedoch gleich 0, da $\sigma_j(b)$ eine Nullstelle von $g^{\sigma_k}(X)$ ist, da $\sigma_k^{-1}\sigma_j(b)$ eine Nullstelle von $g(X)$ ist, da $\sigma_k^{-1}\sigma_j(b)$ eine Nullstelle von $\mu(X)$ ist, die nicht gleich b ist.

Für $r \in [0,\ell-1]$ ist also

$$\hat{\mathrm{Tr}}_{L|K}\Big(g(X)\frac{b^r}{\mu'(b)}\Big) - X^r \;=\; \big(\sum_{k\in[1,\ell]} \hat{\sigma}_k(g(X)\frac{b^r}{\mu'(b)})\big) - X^r \;=\; 0\;,$$

da es sich um ein Polynom in $E[X]$ von Grad $\leqslant \ell-1$ handelt, das beim Einsetzen von $\sigma_j(b)$ gleich 0 wird für $j \in [1,\ell]$. Koeffizientenweise betrachtet wird also $\mathrm{Tr}_{L|K}(c_i\frac{b^r}{\mu'(b)}) - \partial_{r,i} = 0$ für $i \in [0,\ell-1]$. Dies zeigt die *Behauptung.*

Folglich ist $B^{\#,A} = \frac{1}{\mu'(b)}\,{}_A\langle\, c_j \,:\, j \in [0,\ell-1]\,\rangle$; cf. Lemma 31.(3).

Aus $g(X)(X-b) = \mu(X)$ folgt $c_{k-1} - bc_k = a_k$ für $k \in [1,\ell-1]$. Somit ist

$$\begin{array}{lcll}
c_{\ell-1} & = & 1 & = \; b^0 \\
c_{\ell-2} & = & bc_{\ell-1} + a_{\ell-1} & = \; b^1 + b^0 a_{\ell-1} \\
c_{\ell-3} & = & bc_{\ell-2} + a_{\ell-2} & = \; b^2 + b^1 a_{\ell-1} + b^0 a_{\ell-2} \\
c_{\ell-4} & = & bc_{\ell-3} + a_{\ell-3} & = \; b^3 + b^2 a_{\ell-1} + b^1 a_{\ell-2} + b^0 a_{\ell-3} \\
\vdots & & & \\
c_0 & = & bc_1 + a_1 & = \; b^{\ell-1} + b^{\ell-2} a_{\ell-1} + \ldots + b^0 a_1
\end{array}$$

Dies zeigt ${}_A\langle\, c_j \,:\, j \in [0,\ell-1]\,\rangle = {}_A\langle\, b^i \,:\, i \in [0,\ell-1]\,\rangle = B$, da die Erzeuger der jeweils einen Seite dank dieser Gleichungen auch in der anderen Seite liegen. Somit ist $B^{\#,A} = \frac{1}{\mu'(b)}B = (\mu'(b)^{-1})$. Wir erhalten

$$\mathfrak{D}_{L|K,A} \;=\; (B^{\#,A})^{-1} \;=\; (\mu'(b))\;.$$

□

In der Situation von Lemma 97 ist $(\Delta_{L|K,\,(b^i:i\in[0,\ell-1])}) = \mathfrak{d}_{L|K,A} = (\mathrm{N}_{L|K}(\mu'_{b,K}(b)))$; cf. Lemma 96.

Seien σ_j für $j \in [1,\ell]$ wie im vorstehenden Beweis gewählt.

Nun ist $\mu_{b,K}(X) = \prod_{i\in[1,\ell]}(X - \sigma_i(b))$. Also ist $\mu'_{b,K}(X) = \prod_{i\in[2,\ell]}(b - \sigma_i(b))$. Folglich ist

$$\begin{array}{rcl}
\mathrm{N}_{L|K}(\mu'_{b,K}(b)) & = & \prod_{i\in[2,\ell]} \mathrm{N}_{L|K}(b-\sigma_i(b)) \\
& = & \prod_{i\in[2,\ell]} \prod_{j\in[1,\ell]} \sigma_j(b-\sigma_i(b)) \\
& = & \prod_{j\in[1,\ell]} \prod_{i\in[2,\ell]} (\sigma_j(b)-\sigma_j(\sigma_i(b))) \\
& = & \prod_{j\in[1,\ell]} \prod_{k\in[1,\ell]\smallsetminus\{j\}} (\sigma_j(b)-\sigma_k(b))\;,
\end{array}$$

da $(\sigma_j \circ \sigma_i)U$ für $i \in [2,\ell]$ gerade die Nebenklassen ungleich $\sigma_j U$ durchläuft.

Insgesamt wird

$$(\Delta_{L|K,\,(b^i:i\in[0,\ell-1])}) \;=\; (\textstyle\prod_{1\leqslant j<k\leqslant\ell}(\sigma_j(b)-\sigma_k(b))^2)\;,$$

und dies wußten wir schon aus Bemerkung 25.

Definition 98 Für $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(C)$ und $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$ schreiben wir

$$\mathfrak{h}\cdot\mathfrak{g} \;:=\; \mathbf{z}\langle\, h\cdot g \,:\, h\in\mathfrak{h},\; g\in\mathfrak{g}\,\rangle\;;$$

cf. betreffende Konvention, angewandt auf Teilmengen von M.

Bemerkung 99 Sei $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(C)$ und $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$.

Es ist $C\cdot\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(C)$, da mit $\mathfrak{g} = y\cdot\mathfrak{b}$, für geeignete $y \in L^\times$ und $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$, sich $C\cdot\mathfrak{g} = C\cdot y\cdot\mathfrak{b} = y\cdot C\cdot\mathfrak{b}$ ergibt und $C\cdot\mathfrak{b} \in \mathrm{Ideale}^\times(C)$ liegt.

Es ist $(C\cdot\mathfrak{g})^{-1} = C\cdot(\mathfrak{g}^{-1})$ wegen $(C\cdot(\mathfrak{g}^{-1}))\cdot(C\cdot\mathfrak{g}) = (1)$.

Es ist $\mathfrak{h}\cdot\mathfrak{g} = \mathfrak{h}\cdot(C\cdot\mathfrak{g}) \in \underline{\mathrm{Ideale}}^\times(C)$.

Folglich ist $(\mathfrak{h}\cdot\mathfrak{g})^{-1} = (\mathfrak{h}\cdot(C\cdot\mathfrak{g}))^{-1} = \mathfrak{h}^{-1}\cdot(C\cdot\mathfrak{g})^{-1} = \mathfrak{h}^{-1}\cdot C\cdot\mathfrak{g}^{-1} = \mathfrak{h}^{-1}\cdot\mathfrak{g}^{-1}$.

Satz 100 (Transitivität des Diskriminantenideals)
Wir erinnern an den Dedekindbereich A, an $K = \mathrm{Quot}(A)$ perfekt und an die endlichen Körpererweiterungen $M|L|K$ mit den jeweiligen ganzen Abschlüssen $C|B|A$ von A. Hierbei ist $m = [M:L]$ und $\ell = [L:K]$.

(1) *Es ist* $\mathfrak{D}_{M|K,A} = \mathfrak{D}_{M|L,B} \cdot \mathfrak{D}_{L|K,A}$ *; cf. Definitionen* 95.(1) *und* 98.

(2) *Es ist* $\mathfrak{d}_{M|K,A} = \mathrm{N}_{L|K}(\mathfrak{d}_{M|L,B}) \cdot \mathfrak{d}_{L|K,A}^{m}$ *; cf. Definition* 95.(2).

Beachte, daß die rechte Seite von Satz 100.(1) als Produkt gebrochener Ideale aufgefaßt werden kann, wenn man sie $\mathfrak{D}_{M|L,B} \cdot (C \cdot \mathfrak{D}_{L|K,A})$ schreibt; cf. Bemerkung 99.

Beweis.

Ad (1). Wir haben $C^{\#,A} \stackrel{!}{=} C^{\#,B} \cdot B^{\#,A}$ zu zeigen; cf. Bemerkungen 94.(1) und 99.

Wir haben zu zeigen, daß für $\mathfrak{h} \in \underline{\text{Ideale}}^{\times}(C)$ genau dann $\mathfrak{h} \subseteq C^{\#,A}$ liegt, wenn $\mathfrak{h} \subseteq C^{\#,B} \cdot B^{\#,A}$ liegt.

Es ist, cf. Aufgabe 37.(4),

$$\begin{aligned}
\mathfrak{h} \subseteq C^{\#,B} \cdot B^{\#,A} \quad &\Leftrightarrow \quad \mathfrak{h}(B^{\#,A})^{-1} \subseteq C^{\#,B} \\
&\overset{\text{B. 94.(3)}}{\Leftrightarrow} \quad \mathrm{Tr}_{M|L}(\mathfrak{h}(B^{\#,A})^{-1}) \subseteq B \\
&\Leftrightarrow \quad (B^{\#,A})^{-1}\,\mathrm{Tr}_{M|L}(\mathfrak{h}) \subseteq B \\
&\Leftrightarrow \quad \mathrm{Tr}_{M|L}(\mathfrak{h}) \subseteq B^{\#,A} \\
&\overset{\text{B. 94.(3)}}{\Leftrightarrow} \quad \mathrm{Tr}_{L|K}(\mathrm{Tr}_{M|L}(\mathfrak{h})) \subseteq A \\
&\overset{\text{L 19.(1)}}{\Leftrightarrow} \quad \mathrm{Tr}_{M|K}(\mathfrak{h}) \subseteq A \\
&\overset{\text{B. 94.(3)}}{\Leftrightarrow} \quad \mathfrak{h} \subseteq C^{\#,A}\ .
\end{aligned}$$

Ad (2). Es wird

$$\begin{aligned}
\mathfrak{d}_{M|K,A} &\overset{\text{D. 95.(2)}}{=} \mathrm{N}_{M|K}(\mathfrak{D}_{M|K,A}) \\
&\overset{(1)}{=} \mathrm{N}_{M|K}(\mathfrak{D}_{M|L,B} \cdot \mathfrak{D}_{L|K,A}) \\
&= \mathrm{N}_{M|K}(\mathfrak{D}_{M|L,B} \cdot (C \cdot \mathfrak{D}_{L|K,A})) \\
&\overset{\text{L. 88}}{=} \mathrm{N}_{M|K}(\mathfrak{D}_{M|L,B}) \cdot \mathrm{N}_{M|K}(C \cdot \mathfrak{D}_{L|K,A}) \\
&\overset{\text{A. 34.(2)}}{=} \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\mathfrak{D}_{M|L,B})) \cdot \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(C \cdot \mathfrak{D}_{L|K,A})) \\
&\overset{\text{D. 95.(2)}}{=} \mathrm{N}_{L|K}(\mathfrak{d}_{M|L,B}) \cdot \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(C \cdot \mathfrak{D}_{L|K,A})) \\
&\overset{\text{A. 34.(3)}}{=} \mathrm{N}_{L|K}(\mathfrak{d}_{M|L,B}) \cdot \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A}^{m}) \\
&\overset{\text{L. 88}}{=} \mathrm{N}_{L|K}(\mathfrak{d}_{M|L,B}) \cdot \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A})^{m} \\
&\overset{\text{D. 95.(2)}}{=} \mathrm{N}_{L|K}(\mathfrak{d}_{M|L,B}) \cdot \mathfrak{d}_{L|K,A}^{m}\ .
\end{aligned}$$

□

Kapitel 3

Minkowskitheorie

3.1 Gitter in reellen Vektorräumen

Sei $(V, \lfloor -, = \rfloor)$ ein euklidischer Raum, i.e. sei V ein endlichdimensionaler $\mathbf{R}$-Vektorraum und sei $\lfloor -, = \rfloor : V \times V \longrightarrow \mathbf{R}$, $(v, w) \longmapsto \lfloor v, w \rfloor$ eine positiv definite symmetrische Bilinearform, auch als Skalarprodukt auf V bezeichnet. Schreibe $n := \dim_{\mathbf{R}}(V)$. Schreibe $\|v\| := \lfloor v, v \rfloor^{1/2}$ für $v \in V$.

Mittels Gram-Schmidt findet man eine Orthonormalbasis von V. Als euklidischen Raum, und damit auch als metrischen und topologischen Raum, können wir mittels dieser Basis V mit $\mathbf{R}^n$ identifizieren, indem wir einem Vektor aus V seinen Koordinatenvektor bezüglich dieser Basis zuordnen.

Wir erinnern an Cauchy-Schwarz: es ist $|\lfloor v, w \rfloor| \leqslant \|v\| \cdot \|w\|$ für $v, w \in V$. Daraus folgt die Dreiecksungleichung: es ist $\|v + w\| \leqslant \|v\| + \|w\|$ für $v, w \in V$.

Eine Untergruppe der additiven Gruppe von V nennen wir auch kurz eine additive Untergruppe von V.

Definition 101 Ein *Gitter* in V ist eine additive Untergruppe X von V von der Form $X = {}_{\mathbf{Z}}\langle \underline{v} \rangle = {}_{\mathbf{Z}}\langle\, v_i : i \in [1, k] \,\rangle$ für ein $k \geqslant 0$ und für ein $\mathbf{R}$-linear unabhängiges Tupel $\underline{v} = (\, v_i : i \in [1, k] \,)$ von Vektoren in V.

Ein solches Gitter X heißt *voll*, falls $k = n$ ist.

Die Menge

$$\mathrm{Fund}_{\underline{v}}(X) := \{\, \textstyle\sum_{i \in [1,k]} \lambda_i v_i : \lambda_i \in \mathbf{R} \text{ mit } 0 \leqslant \lambda_i \leqslant 1 \text{ für } i \in [1, k] \,\}$$

heißt *Fundamentalbereich* von X bezüglich $\underline{v}$.

Der Begriff des Gitters hier ist nicht zu verwechseln mit dem verwandten, aber verschiedenen Begriff des $\mathbf{Z}$-Gitters aus Aufgabe 18.

Das Gitter $X \subseteq V$ aus Definition 101 ist auch ein $\mathbf{Z}$-Gitter im Sinne von Aufgabe 18, es hat Rang k.

Aber Vorsicht, $\mathbf{z}\langle 1, \sqrt{2}\rangle$ ist ein $\mathbf{Z}$-Gitter, da $(1, \sqrt{2})$ wegen $\sqrt{2} \notin \mathbf{Q}$ ein $\mathbf{Z}$-linear unabhängiges Tupel ist. Dahingegen ist $\mathbf{z}\langle 1, \sqrt{2}\rangle$ kein Gitter in $\mathbf{R}^1$, da ein solches Rang 1 haben muß.

Bemerkung 102 *Sei X ein Gitter in V.*

Die Teilmenge $\mathrm{Fund}_{\underline{v}}(X) \subseteq V$ *ist kompakt, i.e. beschränkt und abgeschlossen.*

Beweis. Nach Identifikation von V mit $\mathbf{R}^n$ als metrischer Raum ist $\mathrm{Fund}_{\underline{v}}(X)$ das Bild der kompakten Teilmenge $\{\, (x_i)_i \in \mathbf{R}^n \,:\, 0 \leqslant x_i \leqslant 1 \text{ für } i \in [1,n] \,\}$ unter einer linearen, also stetigen Abbildung, und also kompakt, und somit abgeschlossen; cf. **[9,** §4.2.1, §4.2.6].

Beschränktheit von $\mathrm{Fund}_{\underline{v}}(X)$ folgt auch direkt aus $\|\sum_{i\in[1,k]}\lambda_i v_i\| \leqslant \sum_{i\in[1,k]}\|v_i\|$ für $\lambda_i \in \mathbf{R}$ mit $0 \leqslant \lambda_i \leqslant 1$ für $i \in [1,k]$. ▫

Bemerkung 103 *Sei X ein volles Gitter in V. Seien $\mathbf{R}$-linear unabhängige Tupel $\underline{v} = (\, v_i \,:\, i \in [1,n]\,)$ und $\underline{w} = (\, w_i \,:\, i \in [1,n]\,)$ mit $X = \mathbf{z}\langle \underline{v}\rangle = \mathbf{z}\langle \underline{w}\rangle$ gegeben.*

(1) *Es ist*
$$\det((\lfloor v_i\,,v_j\rfloor)_{i,j}) \;=\; \det((\lfloor w_i\,,w_j\rfloor)_{i,j})$$

(2) *Sei $\underline{e} = (\, e_i \,:\, i \in [1,n]\,)$ eine Orthonormalbasis von V. Sei $v_j = \sum_{i\in[1,n]} a_{i,j}\, e_i$ für $j \in [1,n]$, mit $A := (a_{i,j})_{i,j} \in \mathbf{R}^{n\times n}$. Dann ist* $\det((\lfloor v_i\,,v_j\rfloor)_{i,j}) = \det(A)^2 \in \mathbf{R}_{>0}$.

Beweis. Sei $G := (\lfloor v_i\,,v_j\rfloor)_{i,j} \in \mathbf{R}^{n\times n}$. Sei $H := (\lfloor w_i\,,w_j\rfloor)_{i,j} \in \mathbf{R}^{n\times n}$.

Ad (1). Schreibe $v_j = \sum_{i\in[1,n]} s_{i,j}\, w_i$ und $w_j = \sum_{i\in[1,n]} t_{i,j}\, v_i$ für $j \in [1,n]$. Sei $S := (s_{i,j})_{i,j}$ und $T := (t_{i,j})_{i,j}$ in $\mathbf{Z}^{n\times n}$. Dann ist $ST = \mathrm{E}_n$, mithin $S \in \mathrm{GL}_n(\mathbf{Z})$.

Für $i,\, j \in [1,n]$ wird
$$\lfloor v_i\,,v_j\rfloor \;=\; \sum_{k,\ell\in[1,n]} s_{k,i}\lfloor w_k\,,w_\ell\rfloor s_{\ell,j}\;.$$

Also ist $G = S^{\mathrm{t}}HS$. Somit ist $\det(G) = \det(S)^2\det(H) = \det(H)$.

Ad (2). Für $i,\, j \in [1,n]$ wird
$$\lfloor v_i\,,v_j\rfloor \;=\; \sum_{k,\ell\in[1,n]} a_{k,i}\lfloor e_k\,,e_\ell\rfloor a_{\ell,j} \;=\; \sum_{k,\ell\in[1,n]} a_{k,i}\,\partial_{k,\ell}\,a_{\ell,j} \;=\; \sum_{k\in[1,n]} a_{k,i}\,a_{k,j}\;.$$

Also ist $G = A^{\mathrm{t}}A$. Somit ist $\det(G) = \det(A)^2$. ▫

Definition 104 Ist X ein volles Gitter in V und ist $\underline{v} = (\, v_i \,:\, i \in [1,n]\,)$ ein $\mathbf{R}$-linear unabhängiges Tupel in V mit $X = \mathbf{z}\langle \underline{v}\rangle$, dann ist, etwas mißbräuchlich notiert,
$$\mathrm{vol}(X) \;:=\; \mathrm{vol}(\mathrm{Fund}_{\underline{v}}(X)) \;\overset{\text{B. 103.(2)}}{=}\; \det((\lfloor v_i\,,v_j\rfloor)_{i,j})^{1/2} \;\in\; \mathbf{R}_{>0}$$
das *Volumen* von X. Dieses hängt nach Bemerkung 103.(1) nicht von der Wahl von $\underline{v}$ ab.

Definition 105 Für $r \in \mathbf{R}_{>0}$ und $w \in V$ sei

$$\mathrm{B}_r(w) \;:=\; \{\, v \in V \,:\, \|v - w\| < r \,\}\,.$$

Eine Teilmenge X von V heißt *diskret,* wenn für $r \in \mathbf{R}_{>0}$ und $w \in V$ die Menge $\mathrm{B}_r(w) \cap X$ endlich ist.

Bemerkung 106

Für eine Teilmenge $X \subseteq V$ sind die folgenden Aussagen $(1, 2)$ äquivalent.

Für eine additive Untergruppe $X \subseteq V$ sind die folgenden Aussagen $(1, 2, 3, 4)$ äquivalent.

(1) *Es ist X eine diskrete Teilmenge von V.*

(2) *Für alle $v \in V$ gibt es ein $\varepsilon \in \mathbf{R}_{>0}$ mit $(\mathrm{B}_\varepsilon(v) \smallsetminus \{v\}) \cap X = \emptyset$.*

(3) *Es gibt ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\mathrm{B}_\varepsilon(0) \cap X = \{0\}$.*

(4) *Es gibt ein $r \in \mathbf{R}_{>0}$ mit $\mathrm{B}_r(0) \cap X$ endlich.*

Beweis. Cf. Aufgabe 41. ▫

Bemerkung 107 *Ist $X \subseteq V$ eine diskrete Teilmenge, dann ist $X \subseteq V$ abgeschlossen.*

Beweis. Für $v \in V \smallsetminus X$ gibt es nach Bemerkung 106.(2) ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\mathrm{B}_\varepsilon(v) \cap X = (\mathrm{B}_\varepsilon(v) \smallsetminus \{v\}) \cap X = \emptyset$. ▫

Lemma 108 *Sei $X \subseteq V$ eine additive Untergruppe.*

Es ist X genau dann ein Gitter in V, wenn X eine diskrete Teilmenge von V ist.

Beweis.

Sei *zum einen* X ein Gitter. Sei ein $\mathbf{R}$-linear unabhängiges Tupel $\underline{v} = (\, v_i \,:\, i \in [1,k]\,)$ so gewählt, daß $X = {}_{\mathbf{Z}}\langle \underline{v} \rangle$ ist. Es ist X ein volles Gitter in $V' := {}_{\mathbf{R}}\langle \underline{v} \rangle$. Ist X diskret in V', dann ist X auch diskret in V; cf. e.g. Bemerkung 106.(3). Somit ist o.E. X ein volles Gitter in V und $k = n$.

Es genügt zu zeigen, daß es ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\mathrm{B}_\varepsilon(0) \cap X = \{0\}$ gibt; cf. Bemerkung 106.(3). Dazu genügt es, ein $\varepsilon \in \mathbf{R}_{>0}$ mit

$$\mathrm{B}_\varepsilon(0) \;\subseteq\; \{\, \textstyle\sum_{i\in[1,n]} \lambda_i v_i \,:\, \lambda_i \in \mathbf{R} \text{ mit } |\lambda_i| < 1 \text{ für } i \in [1,n]\,\}$$

zu finden. Wähle $x_i \in V$ mit $\|x_i\| = 1$ und $\lfloor x_i \,,\, {}_{\mathbf{R}}\langle\, v_1 \,,\, \ldots \,,\, v_{i-1} \,,\, v_{i+1} \,,\, \ldots \,,\, v_n \rangle \rfloor = 0$ für $i \in [1,n]$. Sei $\varepsilon := \min\{\, |\lfloor x_i \,,\, v_i \rfloor| \,:\, i \in [1,n]\,\}$. Es ist $\varepsilon \in \mathbf{R}_{>0}$.

Sei nun $y =: \sum_{i\in[1,n]}\lambda_i v_i \in V$ gegeben mit $\lambda_i \in \mathbf{R}$ und einem $j \in [1,n]$, für welches $|\lambda_j| \geqslant 1$ ist. Mit Cauchy-Schwarz wird

$$\|y\| \;=\; \|y\|\|x_j\| \;\geqslant\; |\lfloor y, x_j\rfloor| \;=\; |\lambda_j\lfloor v_j\,, x_j\rfloor| \;=\; |\lambda_j|\cdot|\lfloor v_j\,, x_j\rfloor| \;\geqslant\; |\lfloor v_j\,, x_j\rfloor| \;\geqslant\; \varepsilon.$$

Also liegt y auch nicht in $\mathrm{B}_\varepsilon(0)$.

Sei *zum anderen* X diskret in V. Sei $V' := {}_{\mathbf{R}}\langle X\rangle$. Ist X ein Gitter in V', dann ist X auch ein Gitter in V. Somit können wir o.E. $V' = V$ annehmen.

Sei nun $\underline{w}$ eine $\mathbf{R}$-lineare Basis von V, deren Elemente in X liegen. Schreibe $Y := {}_{\mathbf{Z}}\langle\underline{w}\rangle$.

Wir wollen zeigen, daß die Faktorgruppe X/Y endlich ist. *Annahme,* nicht. Seien x_i für $i \geqslant 1$ in verschiedenen Nebenklassen gewählt, i.e. sei $x_i - x_j \notin Y$ für alle $i,\, j \geqslant 1$. Sei $y_i \in Y$ so gewählt, daß $x_i - y_i \in \mathrm{Fund}_{\underline{w}}(Y)$ liegt für $i \geqslant 1$, möglich durch ganzzahliges Abrunden der Koeffizienten von x bezüglich $\underline{w}$. Da $\mathrm{Fund}_{\underline{w}}(Y)$ abgeschlossen und beschränkt ist, hat die Folge $(x_i - y_i)_{i\geqslant 1}$ einen Häufungspunkt $z \in \mathrm{Fund}_{\underline{w}}(Y)$; cf. [**9,** §4.2.5, §4.2.6]. Da $X \subseteq V$ abgeschlossen ist nach Bemerkung 107 und da alle Folgenglieder einer gegen z konvergierenden Teilfolge von $(x_i - y_i)_{i\geqslant 1}$ in X liegen, ist auch $z \in X$; denn läge $z \in V \smallsetminus X$, dann gäbe es ein $\eta \in \mathbf{R}_{>0}$ so, daß $\mathrm{B}_\eta(z) \cap X = \emptyset$ ist, was der Konvergenz dieser Teilfolge widerspräche.

Nun gibt es ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\mathrm{B}_\varepsilon(z) \cap X = \{z\}$; cf. Bemerkung 106.(2). Aus der genannten Konvergenz folgt nun, daß es $i,\, j \geqslant 1$ mit $i \neq j$ und $x_i - y_i = z$ und $x_j - y_j = z$ gibt. Aber dann ist $x_i - x_j = y_j - y_i \in Y$, und wir haben einen *Widerspruch* zu $x_i - x_j \notin Y$.

Schreibe $s := |X/Y|$. Es ist $s \cdot (X/Y) = 0$, also $sX \subseteq Y$, also $Y \subseteq X \subseteq \frac{1}{s}Y$. Gemäß Aufgabe 13.(2) ist X endlich erzeugt frei über $\mathbf{Z}$ von Rang n, i.e. $X = {}_{\mathbf{Z}}\langle\underline{v}\rangle$ für ein geeignetes $\underline{v} = (\, v_i \,:\, i \in [1,n]\,)$. Da $V = {}_{\mathbf{R}}\langle X\rangle = {}_{\mathbf{R}}\langle\, {}_{\mathbf{Z}}\langle\underline{v}\rangle\rangle = {}_{\mathbf{R}}\langle\underline{v}\rangle$ ist und da $\dim_{\mathbf{R}}(V) = n$ ist, folgt, daß $\underline{v}$ eine $\mathbf{R}$-lineare Basis von V ist. Somit ist $X \subseteq V$ ein Gitter. ▫

Lemma 109 *Sei $X \subseteq V$ ein Gitter.*

Es ist X genau dann voll, wenn es eine beschränkte Teilmenge $M \subseteq V$ mit

$$V \;=\; \bigcup_{x\in X}(x + M)$$

gibt.

Beweis. Sei $\underline{v}$ ein linear unabhängiges Tupel in V mit $X = {}_{\mathbf{Z}}\langle\underline{v}\rangle$.

Ist X voll, dann ist $V = \bigcup_{x\in X}(x + \mathrm{Fund}_{\underline{v}}(X))$; cf. Bemerkung 102.

Sei umgekehrt $M \subseteq V$ beschränkt mit $V = \bigcup_{x\in X}(x + M)$. Sei $w \in V$. Wir haben $w \overset{!}{\in} {}_{\mathbf{R}}\langle\underline{v}\rangle$ zu zeigen. Letzteres ist eine abgeschlossene Teilmenge in V, wie man wieder nach Identifikation mit $\mathbf{R}^n$ unter Verwendung der Stetigkeit von Linearformen erkennt. Für $i \in \mathbf{Z}_{\geqslant 1}$ können wir $iw = x_i + m_i$ schreiben mit $x_i \in X$ und $m_i \in M$. Dann wird $w = i^{-1}x_i + i^{-1}m_i$ für $i \geqslant 1$. Es ist $i^{-1}x_i \in {}_{\mathbf{R}}\langle\underline{v}\rangle$ für $i \geqslant 1$. Also ist

$$w \;=\; \lim_{i\to\infty} w \;=\; \lim_{i\to\infty}(i^{-1}x_i + i^{-1}m_i) \;=\; \lim_{i\to\infty} i^{-1}x_i \;\in\; {}_{\mathbf{R}}\langle\underline{v}\rangle\,.$$

▫

Lemma 110 (Minkowskischer Gitterpunktsatz)

Sei X ein volles Gitter in V. Wir schreiben weiterhin $n := \dim_{\mathbf{R}} V$.

Sei $M \subseteq V$ eine beschränkte Teilmenge so, daß für m, $m' \in M$ stets $\frac{1}{2}(m-m') \in M$ ist.

Ist $\mathrm{vol}(M) > 2^n \mathrm{vol}(X)$, so ist $\{0\} \subset M \cap X$.

> Die Voraussetzung an die Form von M von Lemma 110 ist e.g. erfüllt, wenn für m, $m' \in M$ stets $-m \in M$ und $\frac{1}{2}(m+m') \in M$ liegen. Das ist e.g. der Fall, wenn M zentralsymmetrisch und konvex ist.

Beweis. Zunächst ist $\mathrm{vol}(M) > 0$, also $M \neq \emptyset$. Wählen wir $m_0 \in M$, so erkennen wir, daß auch $0 = \frac{1}{2}(m_0 - m_0) \in M$ liegt.

Schreibe $X = {}_{\mathbf{Z}}\langle \underline{v} \rangle$ für eine geeignete $\mathbf{R}$-lineare Basis $\underline{v}$ von V.

Es genügt zu zeigen, daß es x, $x' \in X$ mit $x \neq x'$ und $(x + \frac{1}{2}M) \cap (x' + \frac{1}{2}M) \neq \emptyset$ gibt. Denn dann gibt es m, $m' \in M$ mit $x + \frac{1}{2}m = x' + \frac{1}{2}m'$, und es folgt $X \smallsetminus \{0\} \ni x - x' = \frac{1}{2}(m' - m) \in M$.

Annahme, nicht. Dann liegt eine disjunkte Vereinigung $\bigsqcup_{x \in X}(x + \frac{1}{2}M) \subseteq V$ vor. Also haben wir auch $\bigsqcup_{x \in X}((x + \frac{1}{2}M) \cap \mathrm{Fund}_{\underline{v}}(X)) \subseteq \mathrm{Fund}_{\underline{v}}(X)$.

Dabei ist $(x + \frac{1}{2}M) \cap \mathrm{Fund}_{\underline{v}}(X) \neq \emptyset$ nur für endlich viele $x \in X$. Denn da $\mathrm{Fund}_{\underline{v}}(X)$ und M beschränkt sind, gilt dies auch für

$$\mathrm{Fund}_{\underline{v}}(X) + (-\tfrac{1}{2})M \;=\; \{\, y - \tfrac{1}{2}m \;:\; y \in \mathrm{Fund}_{\underline{v}}(X),\, m \in M \,\}\,.$$

Also ist $(\mathrm{Fund}_{\underline{v}}(X) + (-\frac{1}{2})M) \cap X$ endlich; cf. Definition 105, Lemma 108. Desweiteren ist $x \in \mathrm{Fund}_{\underline{v}}(X) + (-\frac{1}{2})M$ äquivalent zu $(x + \frac{1}{2}M) \cap \mathrm{Fund}_{\underline{v}}(X) \neq \emptyset$.

Folglich ist

$$\begin{aligned}
\mathrm{vol}(X) &= \mathrm{vol}(\mathrm{Fund}_{\underline{v}}(X)) \\
&\geqslant \textstyle\sum_{x \in X} \mathrm{vol}(\,(x + \frac{1}{2}M) \cap \mathrm{Fund}_{\underline{v}}(X)\,) \\
&= \textstyle\sum_{x \in X} \mathrm{vol}(\,\frac{1}{2}M \cap (-x + \mathrm{Fund}_{\underline{v}}(X))\,) \\
&= \mathrm{vol}(\tfrac{1}{2}M) \\
&= 2^{-n}\mathrm{vol}(M)\,,
\end{aligned}$$

denn $\bigcup_{x \in X}(-x + \mathrm{Fund}_{\underline{v}}(X)) = V$, und die Schnittmengen der Teilnehmer dieser Vereinigung haben Volumen 0. Wir haben einen *Widerspruch.* ▫

3.2 Endlichkeitsaussagen

Sei $K|\mathbf{Q}$ eine endliche Körpererweiterung, i.e. sei K ein Zahlkörper. Schreibe $k := [K : \mathbf{Q}]$. Sei E ein Zerfällungskörper von $K|\mathbf{Q}$.

Dann ist E Zerfällungskörper eines Polynoms $f(X) \in \mathbf{Q}[X]$; cf. Beweis zu Lemma 11.(2). Schreibe $f(X) = (X - u_1) \cdot (X - u_2) \cdot \ldots \cdot (X - u_n) \in \mathbf{C}[X]$. Sei

$$\tilde{E} \;:=\; \mathbf{Q}(\, u_1 \,,\, u_2 \,,\, \ldots \,,\, u_n \,) \;\subseteq\; \mathbf{C} \;.$$

Dann ist auch $\tilde{E}$ ein Zerfällungskörper von $f(X) \in \mathbf{Q}[X]$; cf. [**5,** §2.5.1]. Also gibt es einen Isomorphismus $\sigma : E \xrightarrow{\sim} \tilde{E}$ mit $\sigma|_{\mathbf{Q}}^{\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$; cf. [**5,** §2.5.3]. Es ist mit $\tilde{K} := \sigma(K)$ auch $\sigma|_K^{\tilde{K}}$ ein Isomorphismus. Es ist $\tilde{E}$ ein Zerfällungskörper von $\tilde{K}|\mathbf{Q}$.

Somit können wir durch Übergang zu einer isomorphen Kopie annehmen, daß $E = \tilde{E}$, $K = \tilde{K}$ und $\mathbf{C}|E|K|\mathbf{Q}$ ist.

Bezeichne $\kappa : \mathbf{C} \to \mathbf{C}$ die komplexe Konjugation. Es ist $E = \kappa(E)$, denn es wird

$$\mathbf{Q}[X] \;\ni\; f(X) \;=\; f^c(X) \;=\; (X - \bar{u}_1) \cdot (X - \bar{u}_2) \cdot \ldots \cdot (X - \bar{u}_n)$$

und also

$$E \;:=\; \mathbf{Q}(\, \bar{u}_1 \,,\, \bar{u}_2 \,,\, \ldots \,,\, \bar{u}_n \,) \;=\; \kappa(E)$$

Für eine Abbildung w von einer Menge M nach E schreiben wir

$$\bar{w}(z) \;:=\; \overline{w(z)} \qquad \text{für } z \in M$$

was unter Beachtung von $E = \kappa(E) \subseteq \mathbf{C}$ eine Abbildung $\bar{w} : M \longrightarrow E$ definiert.

Sei $G := \mathrm{Gal}(E|\mathbf{Q}) \geqslant \mathrm{Gal}(E|K) =: U$. Schreibe $G = \bigsqcup_{\ell \in [1,k]} \rho_\ell U$ mit $\rho_\ell \in G$ für $\ell \in [1,k]$. Sei o.E. $\rho_1 = \mathrm{id}_E$.

Schreiben wir

$$\begin{aligned} \mathrm{Einb}(K) \quad &:= \quad \{\, \rho|_K \,:\, \rho \in G \,\} \;=\; \{\, \rho_\ell|_K \,:\, \ell \in [1,k] \,\} \\ \mathrm{Einb}_{\mathbf{R}}(K) \quad &:= \quad \{\, \rho|_K \,:\, \rho \in G,\, \rho(K) \subseteq \mathbf{R} \,\} \;, \end{aligned}$$

dann ist $|\mathrm{Einb}(K)| = k$; cf. Lemma 15.

Wähle eine Teilmenge $\mathrm{Einb}_{\mathbf{C}}(K) \subseteq \mathrm{Einb}(K) \smallsetminus \mathrm{Einb}_{\mathbf{R}}(K)$ mit

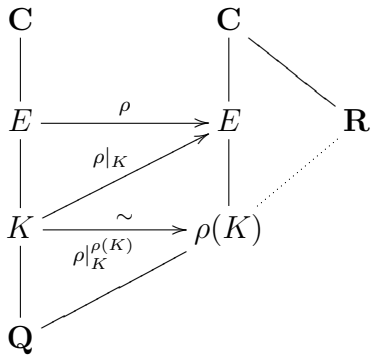
$$\mathrm{Einb}_{\mathbf{R}}(K) \sqcup \bigsqcup_{\sigma \in \mathrm{Einb}_{\mathbf{C}}(K)} \{\, \sigma \,,\, \bar{\sigma} \,\} \;=\; \mathrm{Einb}(K) \;.$$

Schreibe

$$\begin{aligned} r \quad &:= \quad |\mathrm{Einb}_{\mathbf{R}}(K)| \\ s \quad &:= \quad |\mathrm{Einb}_{\mathbf{C}}(K)| \;. \end{aligned}$$

Dann ist $r + 2s = k$.

Mißbräuchlicherweise nennt man die Elemente von $\mathrm{Einb}_{\mathbf{R}}(K)$ auch *reelle*, die von $\mathrm{Einb}_{\mathbf{C}}(K)$ *komplexe* Einbettungen von K.



Beispiel. Sei $K = \mathbf{Q}(\sqrt[3]{2})$. Schreibe $\delta := \sqrt[3]{2}$.

Wir haben $\mathrm{Einb}(K) = \{\, \sigma_j \,:\, j \in [1,3] \,\}$, wobei $\sigma_j : K \longrightarrow E,\ \delta \longmapsto \zeta_3^{j-1}\delta$; cf. Aufgabe 7.(1). Es ist $\mathrm{Einb}_{\mathbf{R}}(K) = \{\sigma_1\}$. Da $\sigma_3 = \bar{\sigma}_2$, können wir $\mathrm{Einb}_{\mathbf{C}}(K) = \{\sigma_2\}$ wählen.

3.2.1 Einbetten eines Zahlkörpers in einen euklidischen Raum

Definition 111

(1) Sei

$$K_{\mathbf{C}} := \prod_{\sigma \in \mathrm{Einb}(K)} \mathbf{C} = \{\, z = (z_\sigma)_\sigma \,:\, z_\sigma \in \mathbf{C} \text{ für } \sigma \in \mathrm{Einb}(K) \,\}\,.$$

Es ist $K_{\mathbf{C}}$ mit eintragsweiser Addition und Multiplikation ein Ring. Es ist $K_{\mathbf{C}}$ mit eintragsweiter Addition und skalarer Multiplikation ein Vektorraum über $\mathbf{C}$.

(2) Wir haben einen injektiven Ringmorphismus

$$\begin{array}{ccc} K & \stackrel{\iota}{\longrightarrow} & K_{\mathbf{C}} \\ x & \longmapsto & (\sigma(x))_{\sigma \in \mathrm{Einb}(K)}\,. \end{array}$$

(3) Sei

$$\begin{array}{ccc} K_{\mathbf{C}} & \stackrel{\mathrm{Tr}}{\longrightarrow} & \mathbf{C} \\ (z_\sigma)_\sigma & \longmapsto & \sum_{\sigma \in \mathrm{Einb}(K)} z_\sigma\,. \end{array}$$

Es ist $\mathrm{Tr}(\iota(x)) = \mathrm{Tr}_{K|\mathbf{Q}}(x)$ für $x \in K$; cf. Lemma 15.(1).

Sei

$$\begin{array}{ccc} K_{\mathbf{C}} & \stackrel{\mathrm{N}}{\longrightarrow} & \mathbf{C} \\ (z_\sigma)_\sigma & \longmapsto & \prod_{\sigma \in \mathrm{Einb}(K)} z_\sigma\,. \end{array}$$

Es ist $\mathrm{N}(\iota(x)) = \mathrm{N}_{K|\mathbf{Q}}(x)$ für $x \in K$; cf. Lemma 15.(2).

(4) Sei

$$\begin{array}{ccccc} K_{\mathbf{C}} & \times & K_{\mathbf{C}} & \stackrel{\lfloor -,= \rfloor}{\longrightarrow} & \mathbf{C} \\ (z & , & w) & \longmapsto & \lfloor z, w \rfloor := \sum_{\sigma \in \mathrm{Einb}(K)} z_\sigma \bar{w}_\sigma\,. \end{array}$$

(5) Sei

$$\begin{array}{rcl} K_{\mathbf{C}} & \xrightarrow{c} & K_{\mathbf{C}} \\ z & \longmapsto & c(z) \ := \ (\bar{z}_{\bar{\sigma}})_{\sigma} \end{array}$$

Es ist $c^2 = \mathrm{id}_{K_{\mathbf{C}}}$. Es ist c ein Ringautomorphismus, da sowohl das Permutieren von Einträgen als auch das eintragsweise Konjugieren mit der 1, mit Addition und mit Multiplikation verträglich sind. Es ist c eine $\mathbf{R}$-lineare Abbildung.

(6) Sei

$$K_{\mathbf{R}} \ := \ \{\, z \in K_{\mathbf{C}} \,:\, c(z) = z \,\} \,.$$

Da c ein Ringautomorphismus ist, ist $K_{\mathbf{R}}$ ein Teilring von $K_{\mathbf{C}}$. Da c eine $\mathbf{R}$-lineare Abbildung ist, ist $K_{\mathbf{R}}$ ein $\mathbf{R}$-linearer Teilraum von $K_{\mathbf{C}}$.

Es ist auch $K_{\mathbf{C}} \simeq K \underset{\mathbf{Q}}{\otimes} \mathbf{C}$ als $\mathbf{C}$-Algebra und $K_{\mathbf{R}} \simeq K \underset{\mathbf{Q}}{\otimes} \mathbf{R}$ als $\mathbf{R}$-Algebra.
Davon wollen wir aber keinen Gebrauch machen.

Bemerkung 112

(1) Es ist

$$K_{\mathbf{R}} \ = \ \{\, z = (z_\sigma)_\sigma \in K_{\mathbf{C}} \,:\, z_\sigma \in \mathbf{R} \text{ für } \sigma \in \mathrm{Einb}_{\mathbf{R}}(K),\ z_{\bar{\sigma}} = \bar{z}_\sigma \text{ für } \sigma \in \mathrm{Einb}_{\mathbf{C}}(K) \,\} \,.$$

Daher hat $K_{\mathbf{R}}$ die $\mathbf{R}$-lineare Basis

$$\begin{array}{rl} & (\, (\partial_{\tau,\sigma})_\sigma \,:\, \tau \in \mathrm{Einb}_{\mathbf{R}}(K) \,) \\ \sqcup & (\, (2^{-1/2}(\partial_{\tau,\sigma} + \partial_{\bar{\tau},\sigma}))_\sigma \,:\, \tau \in \mathrm{Einb}_{\mathbf{C}}(K) \,) \\ \sqcup & (\, (2^{-1/2}(\mathrm{i}\partial_{\tau,\sigma} - \mathrm{i}\partial_{\bar{\tau},\sigma}))_\sigma \,:\, \tau \in \mathrm{Einb}_{\mathbf{C}}(K) \,) \,. \end{array}$$

Insbesondere ist $\dim_{\mathbf{R}}(K_{\mathbf{R}}) = r + 2s = k$.

(2) Sind $z = (z_\sigma)_\sigma$, $w = (w_\sigma)_\sigma \in K_{\mathbf{R}}$, dann ist

$$\begin{array}{rcl} \lfloor z, w \rfloor & = & \big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{R}}(K)} z_\sigma w_\sigma\big) + \big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{C}}(K)} z_\sigma \bar{w}_\sigma\big) + \big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{C}}(K)} z_{\bar{\sigma}} \bar{w}_{\bar{\sigma}}\big) \\ & = & \big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{R}}(K)} z_\sigma w_\sigma\big) + 2\big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{C}}(K)} \mathrm{Re}(z_\sigma \bar{w}_\sigma)\big) \ \in \ \mathbf{R} \,. \end{array}$$

Insbesondere ist

$$\lfloor z, z \rfloor \ = \ \sum_{\sigma \in \mathrm{Einb}(K)} |z_\sigma|^2 \ = \ \Big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{R}}(K)} z_\sigma^2\Big) + 2\Big(\sum_{\sigma \in \mathrm{Einb}_{\mathbf{C}}(K)} |z_\sigma|^2\Big) \in \mathbf{R}_{\geqslant 0} \,,$$

und dies ist genau dann gleich 0, wenn $z = 0$ ist. Somit ist die Einschränkung $\lfloor -, = \rfloor|^{\mathbf{R}}_{K_{\mathbf{R}} \times K_{\mathbf{R}}}$ eine positiv definite symmetrische $\mathbf{R}$-Bilinearform.
Es ist also $(\, K_{\mathbf{R}} \,,\, \lfloor -, = \rfloor|^{\mathbf{R}}_{K_{\mathbf{R}} \times K_{\mathbf{R}}} \,)$ ein euklidischer Raum.
Die in (1) genannte $\mathbf{R}$-lineare Basis ist hierin eine Orthonormalbasis.

(3) Es ist $\iota(K) \subseteq K_{\mathbf{R}} \subseteq K_{\mathbf{C}}$, denn für $x \in K$ ist $\iota(x) = (\rho(x))_{\rho \in \mathrm{Einb}(K)}$, und dabei ist $\overline{\rho(x)} = \overline{\rho}(x)$.

(4) Die Einschränkungen $\mathrm{N}\,|_{K_{\mathbf{R}}}^{\mathbf{R}}$ und $\mathrm{Tr}\,|_{K_{\mathbf{R}}}^{\mathbf{R}}$ existieren und sind stetig; cf. Aufgabe 42.

Beispiel 113 Wir setzen das vorige Beispiel fort.

Darin war $K = \mathbf{Q}(\sqrt[3]{2})$ und $\delta = \sqrt[3]{2}$. Ferner war $\mathrm{Einb}(K) = \{\, \sigma_j \,:\, j \in [1,3] \,\}$, wobei $\sigma_j : K \longrightarrow E$, $\delta \longmapsto \zeta_3^{j-1}\delta$, wobei $\mathrm{Einb}_{\mathbf{R}}(K) = \{\sigma_1\}$ und $\mathrm{Einb}_{\mathbf{C}}(K) = \{\sigma_2\}$

Schreiben wir die Elemente aus $K_{\mathbf{C}}$ als $z = (\, z_{\sigma_1}\,,\, z_{\sigma_2}\,,\, z_{\sigma_3}\,)$, dann wird

$$K_{\mathbf{R}} \;=\; \{\, (\, z_{\sigma_1}\,,\, z_{\sigma_2}\,,\, z_{\sigma_3}\,) \,:\, z_{\sigma_1} \in \mathbf{R},\; z_{\sigma_3} = \bar{z}_{\sigma_2} \,\}$$

ein euklidischer Raum mit

$$\lfloor z, w \rfloor \;=\; z_{\sigma_1} w_{\sigma_1} + 2\,\mathrm{Re}(z_{\sigma_2}\bar{w}_{\sigma_2})$$

und mit Orthonormalbasis

$$\big(\, (1,0,0),\, 2^{-1/2}(0,1,1),\, 2^{-1/2}(0,\mathrm{i},-\mathrm{i})\,\big)\;.$$

3.2.2 Endlichkeit der Klassengruppe

Lemma 114 *Sei* $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathcal{O}_K)$. *Dann ist* $\iota(\mathfrak{a}) \subseteq K_{\mathbf{R}}$ *ein volles Gitter mit*

$$\mathrm{vol}(\iota(\mathfrak{a})) \;=\; |\Delta_K|^{1/2} \cdot |\mathcal{O}_K/\mathfrak{a}|\;.$$

Beweis. Sei $\underline{g} = (\, g_j \,:\, j \in [1,k]\,)$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_K$; cf. Lemma 33.

Sei $\underline{y} = (\, y_i \,:\, i \in [1,k]\,)$ eine $\mathbf{Z}$-lineare Basis von $\mathfrak{a}$, existent, da $\mathbf{Z}$ ein Hauptidealbereich ist; cf. Bemerkung 89. Schreibe $y_i = \sum_{j\in[1,k]} a_{j,i}\, g_j$ mit $(a_{j,i})_{j,i} \in \mathbf{Z}^{k\times k}$. Dann ist $|\mathcal{O}_K/\mathfrak{a}| = |\det(A)|$; cf. Aufgabe 14.(2).

Für $\ell,\, i \in [1,k]$ ist $\rho_\ell(y_i) = \sum_{j\in[1,k]} a_{j,i}\,\rho_\ell(g_j)$ und also $\mathrm{Vand}_{K|\mathbf{Q},\underline{y}} = A^{\mathrm{t}}\,\mathrm{Vand}_{K|\mathbf{Q},\underline{g}}$. Also ist auch

$$\det(\mathrm{Vand}_{K|\mathbf{Q},\underline{y}})^2 \;=\; \det(\mathrm{Vand}_{K|\mathbf{Q},\underline{g}})^2\det(A)^2 \;\overset{\text{L. 24}}{=}\; \Delta_{K|\mathbf{Q},\underline{g}}\det(A)^2 \;=\; \Delta_K \,\cdot\, |\mathcal{O}_K/\mathfrak{a}|^2\;;$$

cf. Definition 37. Insbesondere ist $\det(\mathrm{Vand}_{K|\mathbf{Q},\underline{y}}) \neq 0$; cf. Lemma 22.

Es ist $\iota(\mathfrak{a}) \subseteq K_{\mathbf{R}}$ ein volles Gitter, da $\iota(\mathfrak{a})$ das $\mathbf{Z}$-lineare Erzeugnis von $(\, \iota(y_i) \,:\, i \in [1,k]\,)$ ist, welches eine $\mathbf{R}$-lineare Basis von $K_{\mathbf{R}}$ ist, da es sogar $\mathbf{C}$-linear unabhängig in $K_{\mathbf{C}}$ ist, da $\det((\rho_\ell(y_i))_{i,\ell}) = \det(\mathrm{Vand}_{K|\mathbf{Q},\underline{y}}) \neq 0$ ist.

Für $i,\, j \in [1,k]$ ist

$$\lfloor \iota(y_i)\,, \iota(y_j) \rfloor \;=\; \lfloor (\rho_\ell(y_i))_\ell\,, (\rho_\ell(y_j))_\ell \rfloor \;=\; \sum_{\ell\in[1,k]} \rho_\ell(y_i)\bar{\rho}_\ell(y_j)\;.$$

Also wird

$$\begin{aligned}\operatorname{vol}(\iota(\mathfrak{a}))^2 &\overset{\text{D.104}}{=} \det\left(\left(\lfloor \iota(y_i)\,,\iota(y_j)\rfloor\right)_{i,j}\right)\\ &= \det(\operatorname{Vand}_{K|\mathbf{Q},\underline{y}}\,\overline{\operatorname{Vand}_{K|\mathbf{Q},\underline{y}}}^{\mathrm{t}})\\ &= \det(\operatorname{Vand}_{K|\mathbf{Q},\underline{y}})\cdot\overline{\det(\operatorname{Vand}_{K|\mathbf{Q},\underline{y}})}\\ &= |\det(\operatorname{Vand}_{K|\mathbf{Q},\underline{y}})|^2\\ &= |\det(\operatorname{Vand}_{K|\mathbf{Q},\underline{y}})^2|\\ &= |\Delta_K|\cdot|\mathcal{O}_K/\mathfrak{a}|^2\,.\end{aligned}$$

□

Definition 115 Sei

$$\xi_K \;:=\; \frac{k!}{k^k}\cdot\left(\frac{4}{\pi}\right)^s\cdot|\Delta_K|^{1/2}$$

die *Minkowskischranke* von K.

Lemma 116 *Sei* $\mathfrak{a}\in\operatorname{Ideale}^{\times}(\mathcal{O}_K)$.

Sei $R\in\mathbf{R}_{>0}$ *gegeben mit*

$$R \;>\; k\cdot(\xi_K\cdot|\mathcal{O}_K/\mathfrak{a}|)^{1/k}\,.$$

Dann gibt es ein $a\in\mathfrak{a}^{\times}$ *mit* $\sum_{\sigma\in\operatorname{Einb}(K)}|\sigma(a)|\leqslant R$.

Beweis. Betrachte die Teilmenge $M:=\{\,z\in K_{\mathbf{R}}\;:\;\sum_{\sigma\in\operatorname{Einb}(K)}|z_\sigma|\leqslant R\,\}\subseteq K_{\mathbf{R}}$. Es ist M eine beschränkte Teilmenge, da für $z\in M$ sich stets $|z_\sigma|\leqslant R$ und also $\|z\|^2=\sum_{\sigma\in\operatorname{Einb}(K)}|z_\sigma|^2\leqslant kR^2$ ergibt; cf. Bemerkung 112.(2).

Sind $z,\,z'\in M$, dann ist auch $\frac{1}{2}(z-z')\in M$. Denn dann ist $\sum_{\sigma\in\operatorname{Einb}(K)}|\frac{1}{2}(z_\sigma-z'_\sigma)|\leqslant\frac{1}{2}\sum_{\sigma\in\operatorname{Einb}(K)}(|z_\sigma|+|z'_\sigma|)\leqslant\frac{1}{2}(R+R)=R$.

Schreiben wir $z\in K_{\mathbf{R}}$ als $\mathbf{R}$-Linearkombination in der Orthonormalbasis aus Bemerkung 112.(1, 2), i.e. als

$$z \;=\; \Big(\sum_{\tau\in\operatorname{Einb}_{\mathbf{R}}(K)} a_\tau(\partial_{\tau,\sigma})_\sigma\Big)+\Big(\sum_{\tau\in\operatorname{Einb}_{\mathbf{C}}(K)} u_\tau(2^{-1/2}(\partial_{\tau,\sigma}+\partial_{\bar\tau,\sigma}))_\sigma\Big)+\Big(\sum_{\tau\in\operatorname{Einb}_{\mathbf{C}}(K)} v_\tau(2^{-1/2}(\mathrm{i}\partial_{\tau,\sigma}-\mathrm{i}\partial_{\bar\tau,\sigma}))_\sigma\Big)$$

mit $a_\tau\,,\,u_\tau\,,\,v_\tau\;\in\;\mathbf{R}$ stets, dann ist $z_\tau=a_\tau$, also $|z_\tau|=|a_\tau|$ für $\tau\in\operatorname{Einb}_{\mathbf{R}}(K)$ und $z_\tau=2^{-1/2}(u_\tau+\mathrm{i}v_\tau)$, also $|z_\tau|=2^{-1/2}(u_\tau^2+v_\tau^2)^{1/2}=|\bar z_\tau|=|z_{\bar\tau}|$ für $\tau\in\operatorname{Einb}_{\mathbf{C}}(K)$. Also ist $z\in M$ genau dann, wenn

$$\Big(\sum_{\tau\in\operatorname{Einb}_{\mathbf{R}}(K)}|a_\tau|\Big)+2\cdot2^{-1/2}\Big(\sum_{\tau\in\operatorname{Einb}_{\mathbf{C}}(K)}(u_\tau^2+v_\tau^2)^{1/2}\Big)\;\leqslant\;R$$

ist. Gemäß Aufgabe 45 ist mithin

$$\operatorname{vol}(M)\;=\;2^r\pi^s\,\frac{R^k}{k!}\,.$$

Folglich ist

$$\begin{aligned}\mathrm{vol}(M) &= 2^r\pi^s(k!)^{-1}R^k > 2^r\pi^s(k!)^{-1}k^k\xi_K\cdot|\mathcal{O}_K/\mathfrak{a}| = 2^r\pi^s\left(\tfrac{4}{\pi}\right)^s\cdot|\Delta_K|^{1/2}\cdot|\mathcal{O}_K/\mathfrak{a}| \\ &= 2^k|\Delta_K|^{1/2}\cdot|\mathcal{O}_K/\mathfrak{a}| \overset{\text{L. 114}}{=} 2^k\mathrm{vol}(\iota(\mathfrak{a}))\ .\end{aligned}$$

Nach dem Minkowskischen Gitterpunktsatz, Lemma 110, ist also $\{0\}\subset M\cap\iota(\mathfrak{a})$. Somit gibt es ein $a\in\mathfrak{a}^\times$ mit $\iota(a)\in M$, i.e. mit $\sum_{\sigma\in\mathrm{Einb}(K)}|\sigma(a)|\leqslant R$ für $\sigma\in\mathrm{Einb}(K)$. ▫

Lemma 117 *Sei* $\mathfrak{a}\in\mathrm{Ideale}^\times(\mathcal{O}_K)$.

Es gibt ein $a\in\mathfrak{a}^\times$ *mit* $|\mathrm{N}_{K|\mathbf{Q}}(a)|\leqslant\xi_K\cdot|\mathcal{O}_K/\mathfrak{a}|$.

Beweis. Schreibe

$$R_0 := k\cdot(\xi_K\cdot|\mathcal{O}_K/\mathfrak{a}|)^{1/k}\ .$$

Für jedes $m\geqslant 1$ gibt es ein $a_m\in\mathfrak{a}^\times$ mit $\sum_{\sigma\in\mathrm{Einb}(K)}|\sigma(a_m)|\leqslant R_0+m^{-1}$; cf. Lemma 116.

Für $m\geqslant 1$ ist $\lfloor\iota(a_m),\iota(a_m)\rfloor=\sum_{\sigma\in\mathrm{Einb}(K)}|\sigma(a_m)|^2\leqslant k(R_0+1)^2$; cf. Bemerkung 112.(2). Also hat die Folge $(\iota(a_m))_m$ eine konvergente Teilfolge $(\iota(a_{m_i}))_i$. Diese habe Grenzwert $z\in K_{\mathbf{R}}$. Da $\iota(\mathfrak{a})$ als Gitter in $K_{\mathbf{R}}$ eine diskrete Teilmenge ist, gibt es ein $\varepsilon\in\mathbf{R}_{\geqslant 0}$ mit $(\mathrm{B}_\varepsilon(z)\smallsetminus\{z\})\cap\iota(\mathfrak{a})=\emptyset$; cf. Lemmata 114 und 108, Bemerkung 106.(2). Da aber ein $j\in\mathbf{Z}_{\geqslant 1}$ existiert mit $\iota(a_{m_i})\in\mathrm{B}_\varepsilon(z)$ für $i\in\mathbf{Z}_{\geqslant j}$, muß zum einen $z=\iota(a)$ sein für ein $a\in\mathfrak{a}$, zum anderen muß $a_{m_i}=a$ sein für $i\in\mathbf{Z}_{\geqslant j}$.

Für $m\geqslant 1$ ist

$$\begin{aligned}|\mathrm{N}_{K|\mathbf{Q}}(a_m)| &\overset{\text{D. 111.(3)}}{=} |\mathrm{N}(\iota(a_m))| \\ &= |\textstyle\prod_{\sigma\in\mathrm{Einb}(K)}\sigma(a_m)| \\ &= \textstyle\prod_{\sigma\in\mathrm{Einb}(K)}|\sigma(a_m)| \\ &\overset{\text{A. 46}}{\leqslant} k^{-k}(\textstyle\sum_{\sigma\in\mathrm{Einb}(K)}|\sigma(a_m)|)^k \\ &\leqslant k^{-k}(R_0+m^{-1})^k\ .\end{aligned}$$

Wegen der schließlichen Konstanz unserer Teilfolge erhalten wir

$$|\mathrm{N}_{K|\mathbf{Q}}(a)| \leqslant k^{-k}R_0^k = \xi_K\cdot|\mathcal{O}_K/\mathfrak{a}|\ ;$$

cf. Bemerkung 112.(4). ▫

> Es ist $\mathrm{N}|^{\mathbf{R}}_{K_{\mathbf{R}}}$ stetig; cf. Aufgabe 42. Aber wegen der schließlichen Konstanz der konstruierten Teilfolge ist dies zu wissen noch nicht einmal erforderlich.

Satz 118 (Endlichkeit der Klassengruppe eines Zahlkörpers)

Wir erinnern an die endliche Körpererweiterung $K|\mathbf{Q}$ *mit* $k=[K:\mathbf{Q}]$ *und* $s=|\mathrm{Einb}_{\mathbf{C}}(K)|$, *sowie an ihre Minkowskischranke* $\xi_K=\frac{k!}{k^k}\cdot\left(\frac{4}{\pi}\right)^s\cdot|\Delta_K|^{1/2}$; *cf. Definition* 115.

Wir erinnern an die Klassengruppe $\mathrm{Cl}(\mathcal{O}_K)=\{\,[\mathfrak{g}]:\mathfrak{g}\in\underline{\mathrm{Ideale}}^\times(\mathcal{O}_K)\,\}$, *wobei für* $\mathfrak{g},\tilde{\mathfrak{g}}\in\underline{\mathrm{Ideale}}^\times(\mathcal{O}_K)$ *genau dann* $[\mathfrak{g}]=[\tilde{\mathfrak{g}}]$ *ist, wenn es ein* $x\in K^\times$ *mit* $x\mathfrak{g}=\tilde{\mathfrak{g}}$ *gibt; cf. Definition* 67.

(1) *Für alle* $\mathfrak{g} \in \underline{\text{Ideale}}^\times(\mathcal{O}_K)$ *gibt es ein* $\mathfrak{a} \in \text{Ideale}^\times(\mathcal{O}_K)$ *mit* $|\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K$ *derart, daß* $[\mathfrak{g}] = [\mathfrak{a}]$ *ist.*

(2) *Schreibe* $\{\, p \in \mathbf{Z} \,:\, p \text{ prim und } 2 \leqslant p \leqslant \xi_K \,\} =: \{\, p_i \,:\, i \in [1,\eta] \,\}$*, wobei* η *die Anzahl der Elemente dieser Menge sei.*

Für $i \in [1,\eta]$ *sei* $(p_i) = p_i\mathcal{O}_K = \prod_{j\in[1,d_i]} \mathfrak{q}_{i,j}^{e_{i,j}}$ *die Primidealfaktorzerlegung in* $\mathcal{O}_K$*, wobei* $d_i \geqslant 1$*, wobei* $\mathfrak{q}_{i,j} \in \text{Ideale}^\times_{\text{prim}}(\mathcal{O}_K)$ *und* $e_{i,j} \geqslant 1$ *für* $j \in [1,d_i]$ *und wobei* $\mathfrak{q}_{i,j} \neq \mathfrak{q}_{i,\tilde{j}}$ *für* $j, \tilde{j} \in [1,d_i]$ *mit* $j \neq \tilde{j}$ *; cf. Lemma* 54*, Satz* 63*. Also ist* $(p_i) = \mathbf{Z} \cap \mathfrak{q}_{i,j}$ *für* $j \in [1,d_i]$ *; cf. Aufgabe* 43.(1)*.*

Sei $f_{i,j} := [\mathcal{O}_K/\mathfrak{q}_{i,j} : \mathbf{Z}/(p_i)]$ *für* $i \in [1,\eta]$ *und* $j \in [1,d_i]$*; cf. Aufgabe* 43.(1)*.*

Für $x \in \mathbf{R}_{>0}$ *schreibe* $\text{rund}(x) := 1 + \max\{\, z \in \mathbf{Z} \,:\, z \leqslant x \,\}$ *.*

Dann ist

$$|\text{Cl}(\mathcal{O}_K)| \;\leqslant\; \prod_{i\in[1,\eta]} \prod_{j\in[1,d_i]} \text{rund}\big(\log_{p_i}(\xi_K) f_{i,j}^{-1}\big) \;.$$

(3) *Es ist die Klassengruppe* $\text{Cl}(\mathcal{O}_K)$ *eine abelsche Gruppe endlicher Ordnung.*

Die Schranke aus (2) soll hauptsächlich das Endlichkeitsargument etwas besser faßbar machen. Um sie zu bekommen, muß großzügig Spielraum eingeräumt werden, so daß die erhaltene Schranke praktisch nicht besonders gut brauchbar ist.

Um $\text{Cl}(\mathcal{O}_K)$ zu bestimmen, hilft dagegen oft (1), da dort nicht nur eine Größenaussage, sondern auch eine Aussage über die benötigten Repräsentanten gemacht wird.

Beweis.

Ad (1). Schreibe $\mathfrak{g}^{-1} = x\mathfrak{b}$ mit $x \in K^\times$ und $\mathfrak{b} \in \text{Ideale}^\times(\mathcal{O}_K)$. Es ist $[\mathfrak{b}] = [\mathfrak{g}^{-1}]$.

Wähle $b \in \mathfrak{b}^\times$ mit $|\text{N}_{K|\mathbf{Q}}(b)| \leqslant \xi_K \cdot |\mathcal{O}_K/\mathfrak{b}|$; cf. Lemma 117.

Es ist $\mathfrak{a} := (b)\mathfrak{b}^{-1} \in \text{Ideale}^\times(\mathcal{O}_K)$. Ferner ist $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{g}]$.

Als Ideale von $\mathbf{Z}$ ist

$$\begin{aligned}
(|\mathcal{O}_K/\mathfrak{a}|) &\overset{\text{L. 91}}{=} \text{N}_{K|\mathbf{Q}}(\mathfrak{a}) \\
&\overset{\substack{\text{L. 88} \\ \text{A. 34.(1)}}}{=} \text{N}_{K|\mathbf{Q}}(\,(b)\,)\,\text{N}_{K|\mathbf{Q}}(\mathfrak{b})^{-1} \\
&\overset{\substack{\text{B. 86.(3)} \\ \text{L. 91}}}{=} (\,\text{N}_{K|\mathbf{Q}}(b)\,)(|\mathcal{O}_K/\mathfrak{b}|)^{-1} \\
&= (\,\text{N}_{K|\mathbf{Q}}(b) \cdot |\mathcal{O}_K/\mathfrak{b}|^{-1}) \;.
\end{aligned}$$

Es folgt $|\mathcal{O}_K/\mathfrak{a}| = |\text{N}_{K|\mathbf{Q}}(b)| \cdot |\mathcal{O}_K/\mathfrak{b}|^{-1} \leqslant \xi_K$.

Ad (2). Wir wollen zeigen, daß $\{\, \mathfrak{a} \in \text{Ideale}^\times(\mathcal{O}_K) \,:\, |\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K \,\}$ endlich ist und die Kardinalität dieser Menge nach oben abschätzen. Dies genügt, denn nach (1) ist dann

$$|\text{Cl}(\mathcal{O}_K)| \;\leqslant\; |\{\, \mathfrak{a} \in \text{Ideale}^\times(\mathcal{O}_K) \,:\, |\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K \,\}| \;.$$

Sei $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathcal{O}_K)$ mit $|\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K$ gegeben.

Ist $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathcal{O}_K)$ und $\nu \geqslant 0$ mit $\mathfrak{a} \subseteq \mathfrak{q}^{\nu}$ gegeben, dann ist $\mathrm{N}_{K|\mathbf{Q}}(\mathfrak{q}^{\nu}) = (p^{f\nu})$ mit $(p) := \mathbf{Z} \cap \mathfrak{q}$ und $f := [\mathcal{O}_K/\mathfrak{q} : \mathbf{Z}/(p)]$; cf. Aufgabe 43.(1). Sei o.E. $p > 0$. Es ist

$$p^{f\nu} \overset{\text{L. 91}}{=} |\mathcal{O}_K/\mathfrak{q}^{\nu}| \leqslant |\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K \,.$$

Ist $\nu \geqslant 1$, so folgt $p \leqslant \xi_K$.

Also können wir $\mathfrak{a} = \prod_{i\in[1,\eta]} \prod_{j\in[1,d_i]} \mathfrak{q}_{i,j}^{\nu_{i,j}}$ schreiben, mit $\nu_{i,j} \geqslant 0$ stets und, desweiteren, $p_i^{f_{i,j}\,\nu_{i,j}} \leqslant \xi_K$, i.e. $\nu_{i,j} \leqslant \log_{p_i}(\xi_K) f_{i,j}^{-1}$; für den Wert von $\nu_{i,j}$ gibt es also nur $\mathrm{rund}(\log_{p_i}(\xi_K) f_{i,j}^{-1})$ Möglichkeiten. Somit ist

$$|\{\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathcal{O}_K) \,:\, |\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K \,\}| \leqslant \prod_{i\in[1,\eta]} \prod_{j\in[1,d_i]} \mathrm{rund}\big(\log_{p_i}(\xi_K) f_{i,j}^{-1}\big) \,.$$

Ad (3). Dies folgt aus (2); cf. Definition 67. ▫

Beispiel 119 Sei $K = \mathbf{Q}(\sqrt{-5})$. Schreibe $\alpha := \sqrt{-5}$. Es ist $\mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3.

Es ist $\mathrm{Einb}_{\mathbf{R}}(\mathbf{Q}(\alpha)) = \emptyset$. Es ist $\mathrm{Einb}_{\mathbf{C}}(\mathbf{Q}(\alpha)) := \{\mathrm{id}_{\mathbf{Q}(\alpha)}\}$ wählbar.

Es ist $r = 0$ und $s = 1$.

Ferner ist $\Delta_{\mathbf{Q}(\alpha)} = -20$; cf. Aufgabe 16.(1).

Also ist $\xi_{\mathbf{Q}(\alpha)} = \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right)^1 \cdot |(-20)|^{1/2} = 4\pi^{-1}\sqrt{5} \approx 2{,}847 < 3$. Somit ist, in der Notation von Satz 118.(2), $\eta = 1$ und $p_1 = 2$. Es ist $\log_2(\xi_{\mathbf{Q}(\alpha)}) \approx 1{,}5095$.

Es ist $(2) = (2, \alpha+5)^2 = (2, 1+\alpha)^2$ die Primidealfaktorzerlegung; cf. Aufgabe 30.(3); cf. auch Aufgabe 27.(1). Also ist $d_1 = 1$, $\mathfrak{q}_{1,1} = (2, 1+\alpha)$, $e_{1,1} = 2$ und $f_{1,1} = 1$; letzteres, da $e_{1,1} f_{1,1} = k = 2$ ist gemäß Aufgabe 43.(2).

Folglich ist $|\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\alpha)})| \leqslant \mathrm{rund}(\log_2(\xi_{\mathbf{Q}(\alpha)})) = 2$ dank Satz Satz75.(2).

Man kann auch direkter argumentieren und anführen, daß nun nur die Klassen $[\mathfrak{q}_{1,1}^0]$ und $[\mathfrak{q}_{1,1}^1]$ in $|\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\alpha)})|$ liegen.

Da wir in Aufgabe 27.(1) das Element $[(2, 1+\alpha)]$ der Ordnung 2 in $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\alpha)})$ gefunden haben, folgt $|\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\alpha)})| = 2$; genauer,

$$\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\alpha)}) \;=\; \langle\!\langle\, [(2, 1+\alpha)] \,\rangle\!\rangle \;\simeq\; \mathrm{C}_2 \,.$$

3.2.3 Endliche Erzeugtheit der Einheitengruppe

Lemma 120 *Sei $R \in \mathbf{R}_{>0}$. Schreibe $N_{\leqslant R} := \{\, x \in \mathcal{O}_K^{\times} \,:\, |\mathrm{N}_{K|\mathbf{Q}}(x)| \leqslant R \,\}$.*

Dann gibt es eine endliche Teilmenge $N_{\leqslant R}^0 \subseteq N_{\leqslant R}$ mit der Eigenschaft, daß es für alle $x \in N_{\leqslant R}$ ein $u \in \mathrm{U}(\mathcal{O}_K)$ gibt mit $xu \in N_{\leqslant R}^0$.

Beweis. Schreibe $N_z := \{\, x \in \mathcal{O}_K \,:\, |\mathrm{N}_{K|\mathbf{Q}}(x)| = z \,\}$ für $z \in \mathbf{Z}_{\geqslant 1}$.

Es genügt zu zeigen, daß für jedes $z \in \mathbf{Z}_{\geqslant 1}$ eine endliche Teilmenge $N_z^0 \subseteq N_z$ existiert mit der Eigenschaft, daß es für alle $x \in N_z$ ein $u \in \mathrm{U}(\mathcal{O}_K)$ gibt mit $xu \in N_z^0$. Denn dann können wir $N_{\leqslant R}^0 := \bigcup_{z \in \mathbf{Z}_{\geqslant 1},\, z \leqslant R} N_z^0$ nehmen.

Als abelsche Gruppe ist $\mathcal{O}_K \simeq \mathbf{Z}^{\oplus k}$; cf. Lemma 33. Also ist $\mathcal{O}_K/z\mathcal{O}_K \simeq (\mathbf{Z}/(z))^{\oplus k}$ und somit von Ordnung $|\mathcal{O}_K/z\mathcal{O}_K| = z^k$.

Wähle $N_z^0 \subseteq N_z$ so, daß $\{\, x + z\mathcal{O}_K \,:\, x \in N_z \,\} = \{\, y + z\mathcal{O}_K \,:\, y \in N_z^0 \,\}$ ist mit $y + z\mathcal{O}_K \neq \tilde{y} + z\mathcal{O}_K$ für $y,\, \tilde{y} \in N_z^0$. Insbesondere ist $|N_z^0| \leqslant z^k$.

Sei $x \in N_z$ gegeben, i.e. sei $x \in \mathcal{O}_K$ mit $|\mathrm{N}_{L|K}(x)| = z$. Sei $x + z\mathcal{O}_K = y + z\mathcal{O}_K$ mit $y \in N_z^0$.

Wir haben zu zeigen, daß $\frac{x}{y} \overset{!}{\in} \mathcal{O}_K$ und $\frac{y}{x} \overset{!}{\in} \mathcal{O}_K$ liegen, denn dann folgt $u := \frac{y}{x} \in \mathrm{U}(\mathcal{O}_K)$ und $xu = y \in N_z^0$. Wegen Symmetrie genügt es, $\frac{x}{y} \overset{!}{\in} \mathcal{O}_K$ zu zeigen.

Es ist $x \in y + z\mathcal{O}_K$. Also ist $x = y + \mathrm{N}_{L|K}(y)w$ für ein $w \in \mathcal{O}_K$. Mit $y' := \prod_{\ell \in [2,k]} \rho_\ell(y)$ ist $\mathrm{N}_{L|K}(y) \overset{\text{L. 15.(2)}}{=} yy'$. Es ist $y' \in \mathcal{O}_E$ gemäß Lemma 20.(1). Es ist $y' = \mathrm{N}_{L|K}(y)y^{-1} \in K$. Also ist $y' \in \mathcal{O}_E \cap K = \mathcal{O}_K$. Es folgt

$$\frac{x}{y} \;=\; \frac{y + \mathrm{N}_{L|K}(y)w}{y} \;=\; 1 + wy' \;\in\; \mathcal{O}_K \,.$$

□

Definition 121

Sei $K'_{\mathbf{C}} := \prod_{\sigma \in \mathrm{Einb}(K)} \mathbf{R}$, gesehen als euklidischer Raum mit dem Standardskalarprodukt.

Wir haben den Morphismus abelscher Gruppen

$$\begin{array}{rcl} \mathrm{U}(K_{\mathbf{C}}) & \longrightarrow & K'_{\mathbf{C}} \\ z = (z_\sigma)_\sigma & \longmapsto & \lambda(z) := (\ln|z_\sigma|)_\sigma \,, \end{array}$$

wobei natürlich $\mathrm{U}(K_{\mathbf{C}})$ multiplikativ und $K'_{\mathbf{C}}$ additiv geschrieben wird.

Sei $K'_{\mathbf{R}} := \{\, (w_\sigma)_\sigma \in K'_{\mathbf{C}} \,:\, w_\sigma = w_{\bar{\sigma}} \text{ für } \sigma \in \mathrm{Einb}(K) \,\} \subseteq K'_{\mathbf{C}}$. Es ist $\dim_{\mathbf{R}}(K'_{\mathbf{R}}) = r + s$, da eine $\mathbf{R}$-lineare Basis von $K'_{\mathbf{R}}$ gegeben ist durch

$$(\,(\partial_{\tau,\sigma})_\sigma \,:\, \tau \in \mathrm{Einb}_{\mathbf{R}}(K)\,) \sqcup (\,(\partial_{\tau,\sigma} + \partial_{\bar{\tau},\sigma})_\sigma \,:\, \tau \in \mathrm{Einb}_{\mathbf{C}}(K)\,) \,.$$

Wir haben die Einschränkung

$$\mathrm{U}(K_{\mathbf{R}}) \quad \overset{\lambda_{\mathbf{R}} := \lambda|^{K'_{\mathbf{R}}}_{\mathrm{U}(K_{\mathbf{R}})}}{\longrightarrow} \quad K'_{\mathbf{R}} \,,$$

denn aus $z_{\bar{\sigma}} = \bar{z}_\sigma$ folgt $\ln|z_{\bar{\sigma}}| = \ln|\bar{z}_\sigma| = \ln|z_\sigma|$ für $\sigma \in \mathrm{Einb}(K)$.

Für $w = (w_\sigma)_\sigma \in K'_{\mathbf{C}}$ sei $\mathrm{Tr}(w) = \sum_{\sigma \in \mathrm{Einb}(K)} w_\sigma$. Für $z \in K_{\mathbf{C}}$ ist $\mathrm{Tr}(\lambda(z)) = \ln|\mathrm{N}(z)|$; cf. Definition 111.(3).

Sei $H := \{\, w \in K'_{\mathbf{R}} \,:\, \mathrm{Tr}(w) = 0 \,\} \subseteq K'_{\mathbf{R}}$. Es ist $\dim_{\mathbf{R}}(H) = -1 + \dim_{\mathbf{R}}(K'_{\mathbf{R}}) = r + s - 1$.

Sei $S := \lambda_{\mathbf{R}}^{-1}(H) = \{\, z \in \mathrm{U}(K_{\mathbf{R}}) \,:\, \mathrm{Tr}(\lambda(z)) = 0 \,\} = \{\, z \in K_{\mathbf{R}} \,:\, |\mathrm{N}(z)| = 1 \,\} \leqslant \mathrm{U}(\mathrm{K}_{\mathbf{R}})$. Also haben wir auch die Einschränkung

$$S \xrightarrow{\lambda_{\mathbf{R}}|_S^H} H \ .$$

Wir erinnern an $\iota(K) \subseteq K_{\mathbf{R}}$; cf. Bemerkung 112.(3). Es ist $\iota(\mathrm{U}(\mathcal{O}_K)) \subseteq S$, da für $u \in \mathrm{U}(\mathcal{O}_K)$ sich $\mathrm{N}(\iota(u)) = \mathrm{N}_{K|\mathbf{Q}}(u) \in \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$ ergibt ; cf. Definition 111, Lemma 20.(4).

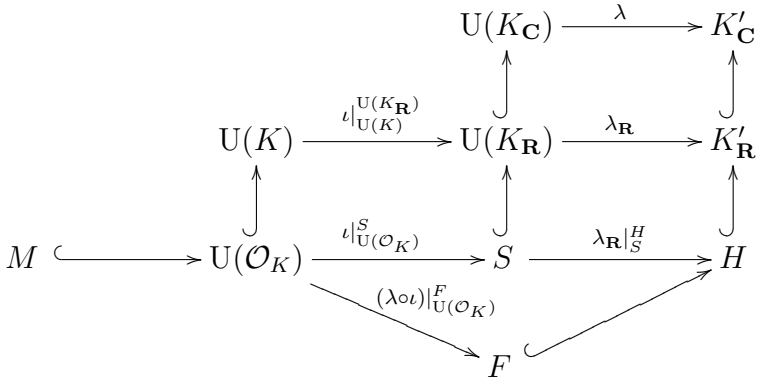
Schreibe

$$\begin{array}{rcl} M & := & \{\, u \in \mathrm{U}(\mathcal{O}_K) \,:\, \lambda(\iota(u)) = 0 \,\} \\ & = & \{\, u \in \mathrm{U}(\mathcal{O}_K) \,:\, |\sigma(u)| = 1 \text{ für } \sigma \in \mathrm{Einb}(K) \,\} \\ & \leqslant & \mathrm{U}(\mathcal{O}_K) \ . \end{array}$$

Schreibe

$$F := \lambda(\iota(\mathrm{U}(\mathcal{O}_K))) \leqslant H \ .$$

So haben wir folgendes kommutative Diagramm von Gruppen und Gruppenmorphismen.



Darin werden die Gruppen F, $K'_{\mathbf{C}}$, $K'_{\mathbf{R}}$, H und F additiv geschrieben, die anderen werden multiplikativ geschrieben.

Bemerkung 122 *Es sind* λ, $\lambda|^{K'_{\mathbf{R}}}_{\mathrm{U}(K_{\mathbf{R}})}$ *und* $\lambda|^H_S$ *surjektiv.*

Beweis. Auf $(w_\tau)_\tau \in K'_{\mathbf{C}}$ bildet e.g. $(\mathrm{e}^{w_\tau})_\tau \in \mathrm{U}(K_{\mathbf{C}})$ ab. Auf $(w_\tau)_\tau \in K'_{\mathbf{R}}$ bildet e.g. $(\mathrm{e}^{w_\tau})_\tau \in \mathrm{U}(K_{\mathbf{R}})$ ab. Schließlich ist $\lambda|^H_S$ dank Urbildkonstruktion surjektiv. ▫

Definition 123 Sei $\mu(K) := \{\, \zeta \in K \,:\, \text{es gibt ein } m \in \mathbf{Z}_{\geqslant 1} \text{ mit } \zeta^m = 1 \,\}$ die Menge der *Einheitswurzeln* in K.

Lemma 124

(1) *Es ist* $\mu(K) = M$.

(2) *Es ist* $\mu(K)$ *eine zyklische endliche Untergruppe von* $\mathrm{U}(\mathcal{O}_K)$.

Beweis. Zu $\mu(K) \overset{!}{\subseteq} M$. Ist $\zeta^m = 1$ für ein $m \in \mathbf{Z}_{\geqslant 1}$, so ist ζ als Nullstelle von $X^m - 1$ in $\mathcal{O}_K$ enthalten. Da $\zeta \cdot \zeta^{m-1} = 1$, ist $\zeta \in \mathrm{U}(\mathcal{O}_K)$. Ferner ist dann auch $|\sigma(\zeta)|^m = |\sigma(\zeta^m)| = 1$ und somit $|\sigma(\zeta)| = 1$ für $\sigma \in \mathrm{Einb}(K)$.

Zu $\mu(K) \overset{!}{\supseteq} M$ und zur Endlichkeit von M. Sei $u \in M$ gegeben, i.e. es ist $u \in \mathrm{U}(\mathcal{O}_K)$ mit $|\sigma(u)| = 1$ für $\sigma \in \mathrm{Einb}(K)$. Also ist $\|\iota(u)\|^2 = \sum_{\sigma \in \mathrm{Einb}(K)} |\sigma(u)|^2 = k$. Somit ist $\iota(u) \in \mathrm{B}_{1+\sqrt{k}}(0)$.

Es ist $\iota(\mathcal{O}_K)$ ein Gitter in $K_{\mathbf{R}}$, also eine diskrete Teilmenge darin; cf. Lemmata 114 und 108. Somit ist $\iota(M)$ als Teilmenge von $\mathrm{B}_{1+\sqrt{k}}(0) \cap \iota(\mathcal{O}_K)$ endlich; cf. Definition 105. Wegen der Injektivität von ι ist also auch M endlich.

Nun ist $\{\, u^i \,:\, i \in \mathbf{Z} \,\}$ als Teilmenge von M endlich. Folglich gibt es $i,\, j \in \mathbf{Z}$ mit $i \neq j$ und $u^i = u^j$, also mit $u^{j-i} = 1$ und folglich mit $u^{|j-i|} = 1$. Also ist $u \in \mu(K)$.

Insgesamt ist die Untergruppe M von $\mathrm{U}(\mathcal{O}_K)$ zum einen gleich $\mu(K)$, zum anderen endlich. Als endliche Untergruppe von $\mathrm{U}(K)$ ist $\mu(K)$ zyklisch; cf. [**5,** Aufgabe 27.(5)]. ▫

Lemma 125 *Es ist* F *ein volles Gitter in* H.

Beweis.

Zeigen wir, daß F *ein Gitter in* H *ist.* Wir haben zu zeigen, daß die Untergruppe F von H diskret ist ; cf. Lemma 108. Es genügt zu zeigen, daß die Untergruppe F von $K'_{\mathbf{R}}$ diskret ist. Es genügt zu zeigen, daß die Schnittmenge $\mathrm{B}_1(0) \cap F$ endlich ist; cf. Bemerkung 106.(4).

Dazu genügt es zu zeigen, daß $\lambda_{\mathbf{R}}^{-1}(\mathrm{B}_1(0)) \cap \iota(\mathrm{U}(\mathcal{O}_K))$ endlich ist. Dazu genügt es zu zeigen, daß $\lambda_{\mathbf{R}}^{-1}(\mathrm{B}_1(0)) \cap \iota(\mathcal{O}_K)$ endlich ist. Da $\iota(\mathcal{O}_K)$ ein Gitter in $K_{\mathbf{R}}$ ist, genügt es zu zeigen, daß $\lambda_{\mathbf{R}}^{-1}(\mathrm{B}_1(0))$ beschränkt ist; cf. Lemmata 114 und 108, Definition 105.

Ist $z \in K_{\mathbf{R}}$ mit $\lambda(z) \in \mathrm{B}_1(0)$ gegeben, dann ist $\|\lambda(z)\|^2 = \sum_{\sigma \in \mathrm{Einb}(K)} (\ln |z_\sigma|)^2 < 1$. Also ist $|z_\sigma| < \mathrm{e}$ für $\sigma \in \mathrm{Einb}(K)$. Folglich ist $\sum_{\sigma \in \mathrm{Einb}(K)} |z_\sigma|^2 < \mathrm{e}^2 k$.

Dies zeigt $\lambda_{\mathbf{R}}^{-1}(\mathrm{B}_1(0)) \subseteq \mathrm{B}_{\mathrm{e}\sqrt{k}}(0)$.

Zeigen wir, daß das Gitter F *in* H *voll ist.* Gemäß Lemma 109 müssen wir eine beschränkte Teilmenge $B \subseteq H$ mit $H = \bigcup_{f \in F} (f + B)$ finden.

Für $c = (c_\sigma)_{\sigma \in \mathrm{Einb}(K)}$ mit stets $c_\sigma \in \mathbf{R}_{>0}$ und $c_\sigma = c_{\bar{\sigma}}$ setzen wir

$$Z_c \;:=\; \{\, z = (z_\sigma)_\sigma \in K_{\mathbf{R}} \,:\, |z_\sigma| \leqslant c_\sigma \text{ für } \sigma \in \mathrm{Einb}(K) \,\} \;\subseteq\; K_{\mathbf{R}} \,.$$

Sind $z,\, \tilde{z} \in Z_c$, dann ist $|\frac{1}{2}(z_\sigma - \tilde{z}_\sigma)| \leqslant \frac{1}{2}|z_\sigma| + \frac{1}{2}|\tilde{z}_\sigma| \leqslant \frac{1}{2}c_\sigma + \frac{1}{2}c_\sigma = c_\sigma$ für $\sigma \in \mathrm{Einb}(K)$ und somit $\frac{1}{2}(z - \tilde{z}) \in Z_c$. Für $z \in Z_c$ ist ferner $\|z\|^2 = \sum_{\sigma \in \mathrm{Einb}(K)} |z_\sigma|^2 \leqslant \sum_{\sigma \in \mathrm{Einb}(K)} c_\sigma^2$ und also $Z_c \subseteq K_{\mathbf{R}}$ eine beschränkte Teilmenge.

Schreiben wir $z \in K_{\mathbf{R}}$ als $\mathbf{R}$-Linearkombination in der Orthonormalbasis aus Bemerkung 112.(1, 2), i.e. als

$$z \;=\; \Big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{R}}(K)} a_\tau(\partial_{\tau,\sigma})_\sigma\Big)+\Big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} u_\tau(2^{-1/2}(\partial_{\tau,\sigma}+\partial_{\bar\tau,\sigma}))_\sigma\Big)+\Big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} v_\tau(2^{-1/2}(\mathrm{i}\partial_{\tau,\sigma}-\mathrm{i}\partial_{\bar\tau,\sigma}))_\sigma\Big)$$

mit $a_\tau\,,\, u_\tau\,,\, v_\tau \;\in\; \mathbf{R}$ stets, dann ist $z_\tau = a_\tau$, also $|z_\tau| = |a_\tau|$ für $\tau \in \mathrm{Einb}_{\mathbf{R}}(K)$ und $z_\tau = 2^{-1/2}(u_\tau + \mathrm{i}v_\tau)$, also $|z_\tau| = 2^{-1/2}(u_\tau^2+v_\tau^2)^{1/2} = |z_{\bar\tau}|$ für $\tau \in \mathrm{Einb}_{\mathbf{C}}(K)$. Also ist $z \in Z_c$ genau dann, wenn

$$\begin{aligned} |a_\tau| &\leqslant c_\tau \quad \text{für } \tau \in \mathrm{Einb}_{\mathbf{R}}(K) \\ 2^{-1/2}(u_\tau^2+v_\tau^2)^{1/2} &\leqslant c_\tau \quad \text{für } \tau \in \mathrm{Einb}_{\mathbf{C}}(K) \end{aligned}$$

ist. Gemäß Aufgabe 45.(1) ist $\mathrm{vol}(Z_c) \;=\; 2^{r+s}\pi^s(\prod_{\tau\in\mathrm{Einb}_{\mathbf{R}}(K)} c_\tau)(\prod_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} c_\tau^2) \;=\; 2^{r+s}\pi^s \prod_{\tau\in\mathrm{Einb}(K)} c_\tau$.

Im Beweis zu Lemma 116 hatten wir unsere Orthonormalbasis in analoger Weise verwendet.

Wähle nun ein solches c so, daß $C := \prod_{\tau\in\mathrm{Einb}(K)} c_\tau > 2^s\pi^{-s}|\Delta_K|^{1/2}$ ist.

Für $y \in \mathrm{U}(K_{\mathbf{R}})$ schreiben wir $c_y := (|y_\sigma|^{-1}c_\sigma)_\sigma$.

Sei $y \in S$. Dann ist $|\mathrm{N}(y)| = 1$ und also $\prod_{\tau\in\mathrm{Einb}(K)} |y_\tau|^{-1}c_\tau = C$. Es ist $\mathrm{vol}(Z_{c_y}) = 2^{r+s}\pi^s C > 2^k|\Delta_K|^{1/2} = 2^k\mathrm{vol}(\iota(\mathcal{O}_K))$; cf. Lemma 114. Also gibt es mit dem Minkowskischen Gitterpunktsatz ein $x_y \in \mathcal{O}_K^\times$ mit $\iota(x_y) \in Z_{c_y}$, i.e. mit $|\sigma(x_y)| \leqslant |y_\sigma|^{-1}c_\sigma$ für $\sigma \in \mathrm{Einb}(K)$; cf. Lemma 110.

Wähle eine endliche Teilmenge $N^0_{\leqslant C} \subseteq N_{\leqslant C} = \{\, x \in \mathcal{O}_K^\times \;:\; |\mathrm{N}_{K|\mathbf{Q}}(x)| \leqslant C \,\}$ mit der Eigenschaft, daß es für alle $x \in N_{\leqslant C}$ ein $u \in \mathrm{U}(\mathcal{O}_K)$ gibt mit $xu \in N^0_{\leqslant C}$; cf. Lemma 120.

Sei

$$T \;:=\; S \,\cap\, \bigcup_{x\in N^0_{\leqslant C}} Z_{c_{\iota(x)}} \;\subseteq\; S \;\subseteq\; K_{\mathbf{R}}\,.$$

Da all diese $Z_{c_{\iota(x)}}$ beschränkt sind, ist auch T beschränkt.

Wir *behaupten,* es ist $\bigcup_{u\in\mathrm{U}(\mathcal{O}_K)} \iota(u)T \stackrel{!}{=} S$. Sei $y \in S$ gegeben. Wir haben zu zeigen, daß es ein $u \in \mathrm{U}(\mathcal{O}_K)$ gibt mit $y \stackrel{!}{\in} \iota(u)T$, i.e. mit $\iota(u)^{-1}y \stackrel{!}{\in} T$.

Es ist $|\mathrm{N}_{K|\mathbf{Q}}(x_y)| = \prod_{\sigma\in\mathrm{Einb}(K)} |\sigma(x_y)| \leqslant \prod_{\sigma\in\mathrm{Einb}(K)} |y_\sigma|^{-1}c_\sigma = C$. Also ist $x_y \in N_{\leqslant C}$. Somit gibt es ein $u_y \in \mathrm{U}(\mathcal{O}_K)$ mit $\hat x := x_y u_y \in N^0_{\leqslant C}$. Es ist $c_{\iota(\hat x)} = (|\sigma(\hat x)|^{-1}c_\sigma)_\sigma$.

Wir wollen $\iota(u_y)^{-1}y \stackrel{!}{\in} T$ zeigen. Es ist $\iota(u_y)^{-1}y \in S$. Wir wollen $\iota(u_y)^{-1}y \stackrel{!}{\in} Z_{c_{\iota(\hat x)}}$ nachweisen, i.e. $|\sigma(u_y)|^{-1}|y_\sigma| \stackrel{!}{\leqslant} |\sigma(\hat x)|^{-1}c_\sigma = |\sigma(x_y)|^{-1}\,|\sigma(u_y)|^{-1}c_\sigma$, i.e. $|y_\sigma| \stackrel{!}{\leqslant} |\sigma(x_y)|^{-1}\,c_\sigma$, i.e. $|\sigma(x_y)| \leqslant |y_\sigma|^{-1}c_\sigma$ für $\sigma \in \mathrm{Einb}(K)$. Aber das ist bekannt und zeigt die *Behauptung.*

Sei $B := \lambda_{\mathbf{R}}(T)$. Es ist T beschränkt. Wähle $R \in \mathbf{R}_{>1}$ mit $T \subseteq \mathrm{B}_R(0)$. Sei $z \in T$. Es ist $\sum_{\sigma\in\mathrm{Einb}(K)} |z_\sigma|^2 = \|z\|^2 < R^2$. Also ist $|z_\sigma| < R$ für $\sigma \in \mathrm{Einb}(K)$. Ferner ist $z \in T \subseteq S$. Also ist $\prod_{\sigma\in\mathrm{Einb}(K)} |z_\sigma| = 1$ und somit $|z_\sigma| > R^{1-k}$ für $\sigma \in \mathrm{Einb}(K)$. Somit ist $\|\lambda_{\mathbf{R}}(z)\|^2 = \sum_{\sigma\in\mathrm{Einb}(K)} (\ln|z_\sigma|)^2 \leqslant k \max\{ (\ln|a|)^2 \ : \ R^{1-k} \leqslant a \leqslant R\} =: R'^2$, mit $R' \in \mathbf{R}_{>0}$. Also ist $B \subseteq \overline{\mathrm{B}}_{R'}(0)$. Folglich ist B beschränkt.

Aus der Behauptung folgt nun

$$H \overset{\text{B.122}}{=} \lambda(S) = \lambda\Big(\bigcup_{u\in\mathrm{U}(\mathcal{O}_K)} \iota(u)T\Big) = \bigcup_{u\in\mathrm{U}(\mathcal{O}_K)} \lambda(\iota(u)T) = \bigcup_{u\in\mathrm{U}(\mathcal{O}_K)} \lambda(\iota(u))+\lambda(T) = \bigcup_{f\in F} f+B\,.$$

□

Satz 126 (Dirichletscher Einheitensatz)

Wir erinnern die endliche Körpererweiterung $K|\mathbf{Q}$.

Wir erinnern an $r := |\mathrm{Einb}_{\mathbf{R}}(K)|$ *und* $s := |\mathrm{Einb}_{\mathbf{C}}(K)|$ *; cf. Beginn von* §3.2.

Wir erinnern an die zyklische endliche Gruppe $\mu(K)$ *der Einheitswurzeln in* K *; cf. Definition* 123*, Lemma* 124.(2).

Wir betrachten die Gruppe $\mu(K) \times \mathbf{Z}^{\oplus(r+s-1)}$. *Sind hierbei* (x, z) *und* $(\tilde{x}, \tilde{z})$ *aus dieser Gruppe, so wird* $(x, z) \cdot (\tilde{x}, \tilde{z}) = (x\tilde{x}, z + \tilde{z})$.

Es gibt einen Gruppenisomorphismus

$$\mathrm{U}(\mathcal{O}_K) \xleftarrow{\sim} \mu(K) \times \mathbf{Z}^{\oplus(r+s-1)}\,,$$

der $(x, 0)$ *auf* x *schickt für* $x \in \mu(K)$.

Insbesondere ist $\mathrm{U}(\mathcal{O}_K)$ *eine endlich erzeugte abelsche Gruppe.*

> Wir kennen in Satz 126 nur die Existenz eines Isomorphismus. Konstruiert haben wir keinen. Das würde die Konstruktion einer $\mathbf{Z}$-linearen Basis von F erfordern, was wir nicht leisten konnten.

Beweis. Es ist $\mu(K)$ der Kern des surjektiven Gruppenmorphismus $\mathrm{U}(\mathcal{O}_K) \xrightarrow{(\lambda\circ\iota)|^F_{\mathrm{U}(\mathcal{O}_K)}} F$; cf. Lemma 124.

Da F ein volles Gitter in H ist und da $\dim_{\mathbf{R}}(H) = r + s - 1$ ist, folgt $F \simeq \mathbf{Z}^{\oplus(r+s-1)}$; cf. Lemma 125, Definition 101.

Also ist $\mathrm{U}(\mathcal{O}_K) \simeq \mu(K) \times \mathbf{Z}^{\oplus(r+s-1)}$; cf. Aufgabe 52.(2).

Da zudem $\mu(K)$ eine endliche Gruppe ist, folgt, daß $\mathrm{U}(\mathcal{O}_K)$ endlich erzeugt ist. □

Beispiel 127

(1) Sei $K = \mathbf{Q}(\sqrt{-5})$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$; cf. Aufgabe 3.

Für $a,\, b \in \mathbf{Z}$ ist $a+b\sqrt{-5} \in \mathrm{U}(\mathbf{Z}[\sqrt{-5}])$ genau dann, wenn $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(a+b\sqrt{-5}) = a^2+5b^2$ in $\mathrm{U}(\mathbf{Z}) = \{-1,+1\}$ liegt; cf. Lemma 20.(4). Dies ist genau dann der Fall, wenn $a \in \{-1,+1\}$ liegt und $b = 0$ ist. I.e. $\mathrm{U}(\mathbf{Z}[\sqrt{-5}]) = \{-1,+1\} \simeq \mathrm{C}_2$.

Betrachten wir nun, was Satz 126 in dieser Situation besagt. Sei nun, genauer gesagt, $\sqrt{-5} = \mathrm{i}\sqrt{5}$. Es ist $r = 0$ und $s = 1$.

Es bildet $\mu(\mathbf{Q}(\sqrt{-5}))$ isomorph nach $\mu(\mathbf{Q}(\sqrt{-5})) \times \mathbf{Z}^{\oplus(0+1-1)}$ und dies isomorph nach $\mathrm{U}(\mathbf{Z}[\sqrt{-5}])$ ab. Dabei kommt x nach $(x,0)$ und sodann nach x. Also ist $\mathrm{U}(\mathbf{Z}[\sqrt{-5}]) = \mu(\mathbf{Q}(\sqrt{-5})) = M$.

Für $a,\, b \in \mathbf{Z}$ ist $|a+b\mathrm{i}\sqrt{5}|^2 = a^2+5b^2$ und $|a-b\mathrm{i}\sqrt{5}|^2 = a^2+5b^2$. Also ist dieses Element $a+b\mathrm{i}\sqrt{5}$ genau dann in M, wenn $a^2+5b^2 = 1$ ist, i.e. wenn $a \in \{-1,+1\}$ und $b = 0$ ist. Es folgt $\mu(\mathbf{Q}(\sqrt{-5})) = M = \{-1,+1\}$; cf. Lemma 124.(1).

Also ist $\mathrm{U}(\mathbf{Z}[\sqrt{-5}]) = \{-1,+1\}$.

(2) Sei $K = \mathbf{Q}(\sqrt{5})$. Schreibe $\alpha := \frac{1}{2}(1+\sqrt{5})$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Es ist $r = 2$ und $s = 0$.

Wir bestimmen $\mu(\mathbf{Q}(\sqrt{5}))$. Ist $z \in \mu(\mathbf{Q}(\sqrt{5}))$, dann können wir ein $m \in \mathbf{Z}_{\geqslant 1}$ wählen mit $z^m = 1$. Also ist $|z|^m = |z^m| = 1$. Da $z \in \mathbf{Q}(\sqrt{5}) \subseteq \mathbf{R}$ liegt, folgt $z \in \{-1,+1\}$. Es folgt $\mu(\mathbf{Q}(\sqrt{5})) = \{-1,+1\} \simeq \mathrm{C}_2$.

Also ist $\mathrm{U}(\mathbf{Z}[\sqrt{5}]) \simeq \mu(\mathbf{Q}(\sqrt{5})) \times \mathbf{Z}^{\oplus(2+0-1)} \simeq \mathrm{C}_2 \times \mathbf{Z}$; cf. Satz 126. Cf. Aufgabe 53.(2).

Kapitel 4

Zerlegung, Verzweigung, Trägheit

4.1 Kreisteilungskörper

Bemerkung 128 *Seien k, $\ell \in \mathbf{Z}_{\geqslant 1}$ teilerfremd. Wähle s, $t \in \mathbf{Z}$ mit $sk + t\ell = 1$.*

(1) *Es sind $\mathbf{Q}(\zeta_k)|\mathbf{Q}$ und $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$ linear disjunkt.*

(2) *Es ist $\mathbf{Q}(\zeta_{k\ell})|\mathbf{Q}$, zusammen mit den Einbettungen, ein Kompositum von $\mathbf{Q}(\zeta_k)|\mathbf{Q}$ und $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$.*

(3) *Wir haben den Gruppenisomorphismus*

$$\begin{array}{rcl} \mathrm{U}(\mathbf{Z}/(k\ell)) & \xrightarrow{\sim} & \mathrm{U}(\mathbf{Z}/(k)) \times \mathrm{U}(\mathbf{Z}/(\ell)) \\ z + (k\ell) & \longmapsto & (z + (k), z + (\ell)) \\ t\ell u + skv + (k\ell) & \longmapsfrom & (u + (k), v + (\ell)) \, . \end{array}$$

Es ist $\varphi(k \cdot \ell) = \varphi(k) \cdot \varphi(\ell)$.

Beweis. Es sind $\mathbf{Q}(\zeta_k)$ und $\mathbf{Q}(\zeta_\ell)$ Teilkörper von $\mathbf{Q}(\zeta_{k\ell})$.

$$\zeta_{k\ell} \;=\; \exp(2\pi\mathrm{i}(k\ell)^{-1})^1 \;=\; \exp(2\pi\mathrm{i}(k\ell)^{-1})^{sk+t\ell} \;=\; \exp(2\pi\mathrm{i}\,\ell^{-1})^s \exp(2\pi\mathrm{i}\,k^{-1})^t \;=\; \zeta_\ell^s \cdot \zeta_k^t \, .$$

Ein Teilkörper von $\mathbf{Q}(\zeta_{k\ell})$, der $\mathbf{Q}(\zeta_k)$ und $\mathbf{Q}(\zeta_\ell)$ enthält, enthält also auch $\zeta_{k\ell}$ und ist damit gleich $\mathbf{Q}(\zeta_{k\ell})$. Also ist $\mathbf{Q}(\zeta_{k\ell})|\mathbf{Q}$ Kompositum von $\mathbf{Q}(\zeta_k)|\mathbf{Q}$ und $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$; cf. Beispiel 41.(1).

Wir haben den surjektiven Ringmorphismus $\mathbf{Z} \longrightarrow \mathbf{Z}/(k) \times \mathbf{Z}/(\ell)$, $z \longmapsto (z + (k), z + (\ell))$; cf. Aufgabe 26.(1). Dieser hat Kern $(k) \cap (\ell)$, was wegen k und ℓ teilerfremd gleich $(k\ell)$ ist. Somit ist $\mathbf{Z}/(k\ell) \simeq \mathbf{Z}/(k) \times \mathbf{Z}/(\ell)$ als Ringe; cf. [**5,** §1.5]. Das gibt den Gruppenisomorphismus $\mathrm{U}(\mathbf{Z}/(k\ell)) \xrightarrow{\sim} \mathrm{U}(\mathbf{Z}/(k) \times \mathbf{Z}/(\ell)) = \mathrm{U}(\mathbf{Z}/(k)) \times \mathrm{U}(\mathbf{Z}/(\ell))$, $z + (k\ell) \longmapsto (z + (k), z + (\ell))$. Sein Inverses ist gegeben durch $t\ell u + skv + (k\ell) \longmapsfrom (u + (k), v + (\ell))$, da dies wohldefiniert ist und da wir $z + (k\ell) = t\ell z + skz + (k\ell) \longmapsfrom (z + (k), z + (\ell))$ erhalten.

Folglich ist $\varphi(k \cdot \ell) = |\mathrm{U}(\mathbf{Z}/(k\ell))| = |\mathrm{U}(\mathbf{Z}/(k))| \cdot |\mathrm{U}(\mathbf{Z}/(\ell))| = \varphi(k) \cdot \varphi(\ell)$. Also ist

$$[\mathbf{Q}(\zeta_{k\ell}) : \mathbf{Q}] \overset{\text{A. 17.(1)}}{=} \varphi(k\ell) = \varphi(k) \cdot \varphi(\ell) \overset{\text{A. 17.(1)}}{=} [\mathbf{Q}(\zeta_k) : \mathbf{Q}] \cdot [\mathbf{Q}(\zeta_\ell) : \mathbf{Q}] .$$

Somit sind $\mathbf{Q}(\zeta_k)|\mathbf{Q}$ und $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$ linear disjunkt; cf. Lemma 44. ▫

Lemma 129 (Kreisteilungsring im Primpotenzfall)

Sei $p \in \mathbf{Z}_{>0}$ eine Primzahl. Sei $\alpha \in \mathbf{Z}_{\geqslant 1}$. Schreibe $q := p^{\alpha-1}$. Beachte $pq = p^\alpha$.

(1) *Es ist $\Phi_{p^\alpha}(X) = \sum_{i\in[0,p-1]} X^{qi}$ und $[\mathbf{Q}(\zeta_{p^\alpha}) : \mathbf{Q}] = \varphi(pq) = (p-1)q$.*

(2) *Es ist $\mathcal{O}_{\mathbf{Q}(\zeta_{p^\alpha})} = \mathbf{Z}[\zeta_{p^\alpha}]$.*

(3) *In $\mathbf{Z}[\zeta_{p^\alpha}]$ ist $(p) = (1-\zeta_{p^\alpha})^{(p-1)q}$ die Primidealfaktorzerlegung im Sinne von Satz 63. Es ist $\mathbf{F}_p \xrightarrow{\sim} \mathbf{Z}[\zeta_{p^\alpha}]/(\zeta_{p^\alpha} - 1)$, $z + (p) \longmapsto z + (\zeta_{p^\alpha} - 1)$ ein Körperisomorphismus.*

(4) *Es ist $|\Delta_{\mathbf{Q}(\zeta_{p^\alpha})}| = p^{q(\alpha p - \alpha - 1)}$.*

Cf. Aufgabe 57 für das Vorzeichen in Lemma 129.(4).

Beweis. Schreibe $\zeta := \zeta_{pq}$. Schreibe $\mathcal{O} := \mathcal{O}_{\mathbf{Q}(\zeta)}$.

Als Nullstelle von $X^{pq} - 1$ liegt $\zeta \in \mathcal{O}$, und somit ist $\mathbf{Z}[\zeta] \subseteq \mathcal{O}$.

Da $X^q - 1 \overset{\text{A. 17.(2)}}{=} \prod_{\beta\in[0,\alpha-1]} \Phi_{p^\beta}(X)$ und $X^{pq} - 1 \overset{\text{A. 17.(2)}}{=} \prod_{\beta\in[0,\alpha]} \Phi_{p^\beta}(X)$ ist, folgt

$$\Phi_{pq}(X) = (X^{pq} - 1)/(X^q - 1) = \sum_{i\in[0,p-1]} X^{qi} .$$

Sodann ist $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \deg(\mu_{\zeta,\mathbf{Q}}) = \deg(\Phi_{pq}) = (p-1)q$; cf. Aufgabe 17. Damit ist (1) gezeigt.

Andererseits ist mit $U := \{\, k \in [0, pq-1] \,:\, k \not\equiv_p 0 \,\}$ auch

$$\Phi_{pq}(X) = \prod_{k+(pq)\in\mathrm{U}(Z/(pq))} (X - \zeta^k) = \prod_{k\in U} (X - \zeta^k) ;$$

cf. Lemma 14, Aufgabe 17.(1).

Zusammengenommen wird

$$p = \sum_{i\in[0,\,p-1]} 1^{qi} = \Phi_{pq}(1) = \prod_{k\in U} (1 - \zeta^k) .$$

Sei $k \in U$. Wähle $\ell \in \mathbf{Z}$ mit $k\ell \equiv_{pq} 1$.

Es ist $\frac{1-\zeta^k}{1-\zeta} \in \mathbf{Z}[\zeta]$. Es ist $(\frac{1-\zeta^k}{1-\zeta})^{-1} = \frac{1-\zeta^{k\ell}}{1-\zeta^k} \in \mathbf{Z}[\zeta]$. Also ist $\frac{1-\zeta^k}{1-\zeta} \in \mathrm{U}(\mathbf{Z}[\zeta]) \leqslant \mathrm{U}(\mathcal{O})$.

Es folgt

$$(p) \;=\; \prod_{k\in U}(1-\zeta^k) \;=\; \prod_{k\in U}((1-\zeta^k)\cdot\tfrac{1-\zeta}{1-\zeta^k}) \;=\; (1-\zeta)^{(p-1)q}$$

als Ideale in $\mathcal{O}$.

Sei nun $(1-\zeta) = \mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_s^{\nu_s}$ die Primidealfaktorzerlegung, wobei $\mathfrak{p}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathcal{O})$ und $\nu_i \geqslant 1$ für $i \in [1,s]$ und wobei $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i,\, j \,\in\, [1,s]$ mit $i \neq j$; cf. Lemma 54, Satz 63. Dann ist

$$(p) \;=\; \mathfrak{p}_1^{(p-1)q\nu_1}\cdots\mathfrak{p}_s^{(p-1)q\nu_s}\;.$$

Schreibe $f_i := [\mathcal{O}/\mathfrak{p}_i : \mathbf{Z}/(p)]$ für $i \in [1,s]$; cf. Aufgabe 43.(1). Es folgt

$$(p-1)q \;=\; \sum_{i\in[1,s]}(p-1)q\,\nu_i\cdot f_i\,;$$

cf. Aufgabe 43.(2). Es folgt $1 = \sum_{i\in[1,s]}\nu_i\,f_i$, also $s=1$, $\nu_1=1$, $\mathfrak{p}_1=(\zeta-1)$ prim und $f_1=1$. Folglich haben wir den Körperisomorphismus

$$\begin{array}{rcl}\mathbf{F}_p = \mathbf{Z}/(p) & \xrightarrow{\sim} & \mathcal{O}/(\zeta-1)\\ z+(p) & \longmapsto & z+(\zeta-1)\;.\end{array}$$

Damit ist unter anderem (2) $\Rightarrow$ (3) gezeigt.

Wir haben die $\mathbf{Z}$-lineare Basis $\underline{z} := (\,\zeta^i \,:\, i\in[0,(p-1)q-1]\,)$ von $\mathbf{Z}[\zeta]$. Es ist

$$\Phi'_{pq}(X) \;=\; (\prod_{k\in U}(X-\zeta^k))' \;=\; \sum_{\ell\in U}\prod_{k\in U\smallsetminus\{\ell\}}(X-\zeta^k)\;,$$

für $m\in U$ also

$$\Phi'_{pq}(\zeta^m) \;=\; \prod_{k\in U\smallsetminus\{m\}}(\zeta^m-\zeta^k)\;.$$

Wir erhalten

$$\begin{array}{rcl}|\Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\,\underline{z}}| & \overset{\text{B. 25}}{=} & |\prod_{k,\,\ell\,\in\,U,\;k<\ell}(\zeta^\ell-\zeta^k)^2|\\ & = & |\prod_{m\in U}\prod_{k\in U\smallsetminus\{m\}}(\zeta^m-\zeta^k)|\\ & = & |\prod_{m\in U}\Phi'_{pq}(\zeta^m)|\\ & \overset{\text{K. 16.(2)}}{=} & |\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\Phi'_{pq}(\zeta))|\;.\end{array}$$

Wäre $\mathcal{O}=\mathbf{Z}[\zeta]$ bereits bekannt, so hätten wir auch $\mathfrak{D}_{\mathbf{Q}(\zeta)|\mathbf{Q}} \overset{\text{L. 97}}{=} (\Phi'_{pq}(\zeta))$ und erhielten damit ebenfalls

$$(\Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\,\underline{z}}) \overset{\text{L. 96}}{=} \mathfrak{d}_{\mathbf{Q}(\zeta)|\mathbf{Q},\mathbf{Z}} \overset{\text{D. 95.(2)}}{=} \mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\mathfrak{D}_{\mathbf{Q}(\zeta)|\mathbf{Q},\mathbf{Z}}) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\Phi'_{pq}(\zeta))\,)\;.$$

Aus $\Phi_{pq}(X)(X^q-1) = X^{pq}-1$ folgt durch formales Ableiten

$$\Phi'_{pq}(X)(X^q-1)+\Phi_{pq}(X)\cdot qX^{q-1} \;=\; pqX^{pq-1}$$

und also

$$\Phi'_{pq}(\zeta) \;=\; \frac{pq\zeta^{-1}}{\zeta^q - 1}\,;$$

cf. [**5,** Aufgabe 11].

Es ist $\mathrm{Gal}(\mathbf{Q}(\zeta^q)|\mathbf{Q}) \simeq \mathrm{U}(\mathbf{Z}/(p))$ und $\mu_{\zeta^q,\mathbf{Q}}(X) = \Phi_p(X) = \frac{X^p-1}{X-1}$; cf. Aufgabe 17. Also wird

$$\prod_{i\in[1,p-1]} (X-(\zeta^{qi}-1)) \overset{\text{L. 14}}{=} \mu_{\zeta^q-1,\mathbf{Q}}(X) \;=\; \mu_{\zeta^q,\mathbf{Q}}(X+1) \;=\; \Phi_p(X+1) \;=\; \frac{(X+1)^p-1}{(X+1)-1} \;=\; \sum_{i\in[0,p-1]} \tbinom{p}{i+1} X^i\,.$$

Vergleich der konstanten Terme gibt

$$|\mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}(\zeta^q-1)| \overset{\text{K. 16.(2)}}{=} |\prod_{i\in[1,p-1]} (\zeta^{qi}-1)| \;=\; p\,.$$

Gemäß Korollar 16.(2) und Lemma 19.(2) ist

$$|\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\zeta^q-1)| \;=\; |\,\mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}(\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}(\zeta^q)}(\zeta^q-1))| \;=\; |\,\mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}((\zeta^q-1)^q)| \;=\; p^q\,.$$

Desweiteren ist $\zeta \in \mathrm{U}(\mathcal{O})$, also $\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\zeta) \in \mathrm{U}(\mathbf{Z})$ und somit $|\,\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\zeta)| = 1$. Es folgt

$$\begin{aligned}
|\Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\underline{z}}| &= |\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\Phi'_{pq}(\zeta))| \\
&= |\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}\left(\frac{pq\zeta^{-1}}{\zeta^q-1}\right)| \\
&= (pq)^{(p-1)q}\cdot p^{-q} \\
&= p^{q(\alpha p-\alpha-1)}\,.
\end{aligned}$$

Dank (1) ist damit (2) $\Rightarrow$ (4) gezeigt.

Es bleibt also (2) zu zeigen. Schreibe $\pi := 1-\zeta$. Oben haben wir den Isomorphismus $\mathbf{Z}/(p) \xrightarrow{\sim} \mathcal{O}/(\pi)$, $z+(p) \longmapsto z+(\pi)$ gesehen. Dessen Surjektivität bedeutet

$$\mathbf{Z} + \pi\mathcal{O} \;=\; \mathcal{O}\,,$$

wobei hier eine Summe von $\mathbf{Z}$-Teilmoduln gebildet wurde. A fortiori ist

$$\mathbf{Z}[\zeta] + \pi\mathcal{O} \;=\; \mathcal{O}\,.$$

Wir *behaupten* $\mathbf{Z}[\zeta] + \pi^t\mathcal{O} \overset{!}{=} \mathcal{O}$ für $t \geqslant 1$. Induktion nach $t \geqslant 1$. Sei $\mathbf{Z}[\zeta] + \pi^t\mathcal{O} = \mathcal{O}$ bekannt. Es folgt

$$\begin{aligned}
\mathbf{Z}[\zeta] + \pi^{t+1}\mathcal{O} &= \mathbf{Z}[\zeta] + \pi\mathbf{Z}[\zeta] + \pi^{t+1}\mathcal{O} \\
&= \mathbf{Z}[\zeta] + \pi(\mathbf{Z}[\zeta] + \pi^t\mathcal{O}) \\
&\overset{\text{I.V.}}{=} \mathbf{Z}[\zeta] + \pi\mathcal{O} \\
&= \mathcal{O}\,.
\end{aligned}$$

Das zeigt die *Behauptung.*

Schreibe $\Delta := |\Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\underline{z}}| = p^{q(\alpha p-\alpha-1)}$. Für $t_0 := (p-1)q \cdot q(\alpha p-\alpha-1)$ ist

$$\pi^{t_0}\mathcal{O} \;=\; (\pi^{(p-1)q}\mathcal{O})^{q(\alpha p-\alpha-1)} \;=\; (p\mathcal{O})^{q(\alpha p-\alpha-1)} \;=\; \Delta\mathcal{O}\,,$$

sodaß vorstehende Behauptung

$$\mathbf{Z}[\zeta] + \Delta\mathcal{O} \;=\; \mathcal{O}$$

liefert. Es bleibt zu zeigen, daß $\Delta\mathcal{O} \subseteq \mathbf{Z}[\zeta]$ liegt. Es ist

$$\mathbf{Z}[\zeta] \;\subseteq\; \mathcal{O} \;\subseteq\; \mathcal{O}^{\#} \;\subseteq\; \mathbf{Z}[\zeta]^{\#}\,;$$

cf. Bemerkung 30, Lemma 31.(2). Wegen $\mathbf{Z}[\zeta] = {}_{\mathbf{Z}}\langle\underline{z}\rangle$ ist

$$|\mathbf{Z}[\zeta]^{\#}/\mathbf{Z}[\zeta]| \;\overset{\text{A. 14.(3)}}{=}\; |\Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\underline{z}}| \;=\; \Delta\,.$$

Es folgt $\Delta \cdot (\mathbf{Z}[\zeta]^{\#}/\mathbf{Z}[\zeta]) = 0$, mithin

$$\Delta\mathcal{O} \;\subseteq\; \Delta\mathbf{Z}[\zeta]^{\#} \;\subseteq\; \mathbf{Z}[\zeta]\,.$$

Damit ist $\mathbf{Z}[\zeta] = \mathcal{O}$, was (2) zeigt.

Bemerkung. Sei $m \in \mathbf{Z}_{\geqslant 1}$ mit $m \equiv_2 1$ gegeben.

Seien $s,\, t \in \mathbf{Z}$ gewählt mit $2s + mt = 1$. Insbesondere ist $t \equiv_2 1$.

Dann ist $\zeta_{2m} = \zeta_{2m}^{2s+mt} = \zeta_m^s \cdot \zeta_2^t = \zeta_m^s \cdot (-1)^t = -\zeta_m^s \in \mathbf{Q}(\zeta_m)$. Also ist $\mathbf{Q}(\zeta_{2m}) = \mathbf{Q}(\zeta_m)$.

Betrachtet man für $n \in \mathbf{Z}_{\geqslant 1}$ den Kreisteilungskörper $\mathbf{Q}(\zeta_n)$, so kann man sich folglich auf den Fall $\mathrm{v}_2(n) \neq 1$ beschränken.

Satz 130 (Kreisteilungsring)

Sei $n \in \mathbf{Z}_{\geqslant 1}$ mit $\mathrm{v}_2(n) \neq 1$.

(1) *Es ist $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$.*

(2) *Sei $P_n := \{\, p \in \mathbf{Z}_{>0} \,:\, p$ ist prim und $n \equiv_p 0 \,\}$ die Menge der Primteiler von n.*
Für $p \in \mathbf{Z}_{>0}$ prim schreiben wir $n[p] := p^{\mathrm{v}_p(n)}$.
Es ist $\Delta_{\mathbf{Q}(\zeta_n)} = \prod_{p\in P_n} \Delta_{\mathbf{Q}(\zeta_{n[p]})}^{\varphi(n/n[p])}$; cf. Lemma 129.(4).
Es ist P_n auch die Menge der Primteiler von $\Delta_{\mathbf{Q}(\zeta_n)}$.

Beweis. Wir führen eine Induktion über $|P_n|$. Als Induktionsanfang verwenden wir, daß wir die Aussagen im Falle $|P_n| \leqslant 1$ aus Lemma 129 kennen. Man beachte insbesondere, daß im Falle $n = p^\alpha$ mit $p \geqslant 2$ prim und $\alpha \geqslant 1$ aus $\mathrm{v}_2(n) \neq 1$ folgt, daß $p \geqslant 3$ oder $\alpha \geqslant 2$ ist und daher jedenfalls $\alpha p - \alpha - 1 \geqslant 1$ ist, mithin $\Delta_{\mathbf{Q}(\zeta_{p^\alpha})} \equiv_p 0$.

Sei $|P_n| \geqslant 2$. Schreibe $n = k\ell$ mit $k, \ell \in \mathbf{Z}_{\geqslant 2}$ teilerfremd. Dann ist $|P_k| < |P_n|$ und $|P_\ell| < |P_n|$. Ferner ist $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ ein Kompositum der linear disjunkten Körpererweiterungen $\mathbf{Q}(\zeta_k)|\mathbf{Q}$ und $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$; cf. Bemerkung 128.(1, 2)

Nach Induktion ist P_k die Menge der Primteiler von $\Delta_{\mathbf{Q}(\zeta_k)}$ und P_ℓ die Menge der Primteiler von $\Delta_{\mathbf{Q}(\zeta_\ell)}$, und es ist $P_k \cap P_\ell = \emptyset$. Also sind $\Delta_{\mathbf{Q}(\zeta_k)}$ und $\Delta_{\mathbf{Q}(\zeta_\ell)}$ teilerfremd.

Folglich können wir Satz 48 anwenden. Wir erhalten mit Induktion

$$\begin{aligned}
\Delta_{\mathbf{Q}(\zeta_n)} &\overset{\text{S. 48.(2)}}{=} \Delta_{\mathbf{Q}(\zeta_k)}^{\varphi(\ell)} \cdot \Delta_{\mathbf{Q}(\zeta_\ell)}^{\varphi(k)} \\
&\overset{\text{I.V.}}{=} \left(\prod_{p\in P_k} \Delta_{\mathbf{Q}(\zeta_{k[p]})}^{\varphi(k/k[p])}\right)^{\varphi(\ell)} \cdot \left(\prod_{p\in P_\ell} \Delta_{\mathbf{Q}(\zeta_{\ell[p]})}^{\varphi(\ell/\ell[p])}\right)^{\varphi(k)} \\
&\overset{\text{B. 128.(3)}}{=} \left(\prod_{p\in P_k} \Delta_{\mathbf{Q}(\zeta_{k[p]})}^{\varphi(n/k[p])}\right) \cdot \left(\prod_{p\in P_\ell} \Delta_{\mathbf{Q}(\zeta_{\ell[p]})}^{\varphi(n/\ell[p])}\right) \\
&= \prod_{p\in P_n} \Delta_{\mathbf{Q}(\zeta_{n[p]})}^{\varphi(n/n[p])}
\end{aligned}$$

cf. Aufgabe 17.(1).

Es ist $\mathcal{O}_{\mathbf{Q}(\zeta_n)} \supseteq \mathbf{Z}[\zeta_n]$, da ζ_n in $\mathbf{Q}(\zeta_n)$ eine Nullstelle von $X^n - 1$ ist.

Zu zeigen ist $\mathcal{O}_{\mathbf{Q}(\zeta_n)} \overset{!}{\subseteq} \mathbf{Z}[\zeta_n]$. Ist $\underline{g'}$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\zeta_k)} \overset{\text{I.V.}}{=} \mathbf{Z}[\zeta_k]$ und $\underline{g''}$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\zeta_\ell)} \overset{\text{I.V.}}{=} \mathbf{Z}[\zeta_\ell]$, dann ist $(\, g'_i g''_j \,:\, i \in [1, \varphi(k)],\ j \in [1, \varphi(\ell)]\,)$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$; cf. Satz 48.(2). Da $\mathbf{Z}[\zeta_k] \subseteq \mathbf{Z}[\zeta_n]$ und $\mathbf{Z}[\zeta_\ell] \subseteq \mathbf{Z}[\zeta_n]$, ist auch $g'_i g''_j \in \mathbf{Z}[\zeta_n]$ stets und folglich $\mathcal{O}_{\mathbf{Q}(\zeta_n)} \subseteq \mathbf{Z}[\zeta_n]$. ▫

Satz 131 (Primidealfaktorzerlegung in Kreisteilungsringen)

Sei $n \in \mathbf{Z}_{\geqslant 1}$ mit $\mathrm{v}_2(n) \neq 1$.

Sei $p \in \mathbf{Z}_{>0}$ prim. Wir schreiben $n[p] := p^{\mathrm{v}_p(n)}$.

Sei $e := \varphi(n[p])$.

Sei $f := |\langle\!\langle p + (n/n[p])\rangle\!\rangle|$ die Ordnung der Restklasse von p in $\mathrm{U}(\mathbf{Z}/(n/n[p]))$.

Sei $d := \varphi(n/n[p])/f$; cf. [**5,** Aufgabe 11.(1.c)].

Für $g(X) \in \mathbf{Z}[X]$ schreiben wir $\bar{g}(X)$ für sein Bild unter der koeffizientenweise angewandten Restklassenabbildung $\mathbf{Z} \longrightarrow \mathbf{F}_p$.

Die Faktorisierung von $\bar{\Phi}_n(X)$ in normierte irreduzible Faktoren in $\mathbf{F}_p[X]$ ist von der Form

$$\bar{\Phi}_n(X) \;=\; \prod_{i\in[1,d]} \bar{g}_i(X)^e$$

für geeignete normierte Polynome $g_i(X) \in \mathbf{Z}[X]$ mit $\deg(g_i) = f$, mit $\bar{g}_i(X)$ irreduzibel und mit $\bar{g}_i(X) \neq \bar{g}_j(X)$ für $i, j \in [1, d]$ mit $i \neq j$.

In $\mathbf{Z}[\zeta_n]$ haben wir die Primidealfaktorzerlegung im Sinne von Satz 63

$$(p) \;=\; \prod_{i\in[1,d]} (g_i(\zeta_n),\, p)^e$$

mit $\mathfrak{q}_i := (g_i(\zeta_n),\, p) \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\zeta_n])$ *für* $i \in [1,d\,]$, *wobei* $\mathfrak{q}_i \neq \mathfrak{q}_j$ *für* $i,\, j \,\in\, [1,d\,]$ *mit* $i \neq j$. *Ferner ist*

$$[\mathbf{Z}[\zeta_n]/\mathfrak{q}_i : \mathbf{F}_p] = f$$

für $i \in [1,d\,]$.

Beweis. Schreibe $\zeta := \zeta_n$. Schreibe $q := n[p]$. Schreibe $m := n/q$. Für $k \in \mathbf{Z}_{\geqslant 1}$ schreiben wir $U_k := \{\, z \in [0,k-1] \,:\, (z)+(k) = (1)\,\}$, sodaß $\mathrm{U}(\mathbf{Z}/(k)) = \{\, z+(k) \,:\, z \in U_k\,\}$ ist.

Faktorisiere

$$\bar{\Phi}_n(X) \;=\; \prod_{i\in[1,\tilde{d}\,]} \bar{g}_i(X)^{e_i} \;\in\; \mathbf{F}_p[X]$$

mit $\tilde{d} \geqslant 1$, mit $e_i \geqslant 1$, $g_i(X) \in \mathbf{Z}[X]$ normiert, $\bar{g}_i(X) \in \mathbf{F}_p[X]$ irreduzibel für $i \in [1,\tilde{d}\,]$ und mit $\bar{g}_i(X) \neq \bar{g}_j(X)$ für $i,\, j \,\in\, [1,\tilde{d}\,]$ mit $i \neq j$.

Schreibe $\mathfrak{q}_i := (g_i(\zeta), p)$ für $i \in [1,\tilde{d}\,]$. Es ist

$$(p) \;=\; \prod_{i\in[1,\tilde{d}\,]} \mathfrak{q}_i^{e_i}$$

die Primidealfaktorzerlegung in $\mathbf{Z}[\zeta]$, und dabei ist der Restklassenkörper $\mathbf{Z}[\zeta]/\mathfrak{q}_i \;\simeq\; \mathbf{F}_p[X]/(\bar{g}_i(X))$ von Grad $\deg(g_i)$ über $\mathbf{F}_p$ für $i \in [1,\tilde{d}\,]$; cf. Lösung zu Aufgabe 30.(2).

Wir haben $\tilde{d} \stackrel{!}{=} d$, $e_i \stackrel{!}{=} e$ und $\deg(\bar{g}_i) \stackrel{!}{=} f$ für $i \in [1,\tilde{d}\,]$ zu zeigen.

Wähle $s,\, t \,\in\, \mathbf{Z}$ mit $sq + tm = 1$. Beachte $(sq)+(m) = (1)$. Es ist

$$\begin{array}{ccccc} \mathrm{U}(\mathbf{Z}/(q)) & \times & \mathrm{U}(\mathbf{Z}/(m)) & \xrightarrow{\sim} & \mathrm{U}(\mathbf{Z}/(n)) \\ (u+(q) & , & v+(m)) & \longmapsto & tmu+sqv+(n)\,; \end{array}$$

cf. Bemerkung 128.(3). Also ist $\mathrm{U}(\mathbf{Z}/(n)) \;=\; \{\, tmu+sqv+(n) \,:\, u \in U_q\,,\; v \in U_m\,\}$, dank Lemma 14 und Aufgabe 17.(1) also

$$\Phi_n(X) \;=\; \prod_{u\in U_q} \prod_{v\in U_m} (X - \zeta^{tmu+sqv})\;.$$

Da $(\mathbf{Z}[\zeta]/\mathfrak{q}_1) \,|\, (\mathbf{Z}/(p)) = \mathbf{F}_p$, ist $\mathrm{char}(\mathbf{Z}[\zeta]/\mathfrak{q}_1) = p$, also $0 = \zeta^{tmuq} - 1 \equiv_{\mathfrak{q}_1} (\zeta^{tmu}-1)^q$ und daher $0 \equiv_{\mathfrak{q}_1} \zeta^{tmu} - 1$ stets; cf. [**5,** Aufgabe 24.(1)]. Somit wird

$$\Phi_n(X) \;=\; \prod_{u\in U_q} \prod_{v\in U_m} (X - \zeta^{tmu+sqv}) \;\equiv_{\mathfrak{q}_1}\; \prod_{u\in U_q} \prod_{v\in U_m} (X - \zeta^{sqv}) \;=\; \prod_{u\in U_q} \Phi_m(X) \;=\; \Phi_m(X)^{\varphi(q)}\;.$$

Da $\mathfrak{q}_1 \cap \mathbf{Z} \;=\; (p)$ ist, folgt hieraus $\Phi_n(X) \;\equiv_p\; \Phi_m(X)^{\varphi(q)}$, i.e. $\bar{\Phi}_n(X) \;=\; \bar{\Phi}_m(X)^e$; cf. Aufgabe 43.(1).

Da f und d beim Übergang von n zu m unverändert bleiben und da dabei e zu 1 wird, können wir nun o.E. $n = m$ annehmen, i.e. $n \not\equiv_p 0$.

Sei $i \in [1, \tilde{d}]$. Schreibe $F_i := \mathbf{Z}[\zeta]/\mathfrak{q}_i$. Es ist $F_i|\mathbf{F}_p$ eine endliche Körpererweiterung; cf. Aufgabe 43.(1).

Für $z \in \mathbf{Z}[\zeta]$ schreiben wir $\bar{z} := z + \mathfrak{q}_i \in F_i$. Nach Konstruktion ist $F_i = \mathbf{F}_p(\bar{\zeta})$. Es ist $\mathbf{F}_p[X] \subseteq F_i[X]$, sodaß wir auch $\bar{\Phi}_n(X) \in F_i[X]$ wiederfinden, etc.

Wir haben $\tilde{d} \stackrel{!}{=} d$, $e_i \stackrel{!}{=} 1$ und $\deg(\bar{g}_i) = [F_i : \mathbf{F}_p] \stackrel{!}{=} f$ zu zeigen.

Es zerfällt $X^n - 1$ in $\mathbf{Z}[\zeta][X]$ in

$$X^n - 1 \;=\; \prod_{k\in[0,n-1]} (X - \zeta^k)$$

und also in $F_i[X]$ in

$$X^n - \bar{1} \;=\; \prod_{k\in[0,n-1]} (X - \bar{\zeta}^k)\;.$$

Wäre einer dieser Linearfaktoren dort mit Exponent $\geqslant 2$ vertreten, so wäre er nicht nur ein Teiler von $X^n - \bar{1}$ sondern auch ein Teiler von $(X^n - \bar{1})'$ in $F_i[X]$. Aber $(X^n - \bar{1})' = \bar{n}X^{n-1}$ hat wegen $n \not\equiv_p 0$ und also $\bar{n} \neq 0$ in F_i nur den irreduziblen Teiler X, was wiederum kein Teiler von $X^n - \bar{1}$ ist. *Widerspruch.* Also gilt $\zeta^k \not\equiv_{\mathfrak{q}_i} \zeta^\ell$ für $k, \ell \in [0, n-1]$, anders gesagt, es sind die Potenzen $\bar{\zeta}^k$ für $k \in [0, n-1]$ in F_i paarweise verschieden. I.e. es ist $|\langle\!\langle \bar{\zeta} \rangle\!\rangle| = n$.

Es ist in $F_i[X]$ ferner $\bar{\Phi}_n(X)$ ein Teiler von $X^n - \bar{1}$. *Wäre* in der Faktorisierung $\bar{\Phi}_n(X) \;=\; \prod_{j\in[1,\tilde{d}]} \bar{g}_j(X)^{e_j}$ in $\mathbf{F}_p[X] \subseteq F_i[X]$ nun $e_i \geqslant 2$, so würde in der Faktorisierung $X^n - \bar{1} \;=\; \prod_{k\in[0,n-1]}(X - \bar{\zeta}^k)$ in $F_i[X]$ ein Linearfaktor mit Exponent $\geqslant 2$ auftreten, was aber *nicht* der Fall ist. Also ist $e_i = 1$.

Sei $z \in \mathbf{Z}[\zeta]$ mit $\bar{z} \neq 0$ gegeben. Wir *behaupten,* daß genau dann $\bar{\Phi}_n(\bar{z}) = 0$ ist, wenn $|\langle\!\langle \bar{z} \rangle\!\rangle| = n$ ist.

Gemäß Aufgabe 17.(2) ist

$$X^n - \bar{1} \;=\; \prod_{s\in[1,n],\; n\equiv_s 0} \bar{\Phi}_s(X) \;\in\; F_i[X]\;.$$

Sei $\bar{\Phi}_n(\bar{z}) = 0$. Dann ist $\bar{z}^n - \bar{1} = 0$. Da ferner $X^n - \bar{1}$ in ein Produkt paarweise verschiedener Linearfaktoren zerfällt, folgt $\bar{\Phi}_s(\bar{z}) \neq 0$ für alle $s \in [1, n-1]$ mit $n \equiv_s 0$. Ist nun $s \in [1, n-1]$ mit $n \equiv_s 0$ gegeben, so zerfällt

$$X^s - \bar{1} \;=\; \prod_{t\in[1,s],\; s\equiv_t 0} \bar{\Phi}_t(X) \;\in\; F_i[X]\;.$$

Es folgt $\bar{z}^s - \bar{1} = \prod_{t\in[1,s],\; s\equiv_t 0} \bar{\Phi}_t(\bar{z}) \neq 0$, da all diese Faktoren nicht verschwinden. Somit ist $|\langle\!\langle \bar{z} \rangle\!\rangle| = n$.

Sei umgekehrt $|\langle\!\langle \bar{z} \rangle\!\rangle| = n$. Dann ist $\bar{z}^n - \bar{1} = 0$. *Wäre* $\bar{\Phi}_s(\bar{z}) = 0$ für ein $s \in [1, n-1]$ mit $n \equiv_s 0$, dann wäre auch $\bar{z}^s - \bar{1} = 0$ und also $|\langle\!\langle \bar{z} \rangle\!\rangle|$ ein Teiler von s, was *nicht* der Fall ist; cf. [**5,** Aufgabe 27.(1)]. Also muß $\bar{\Phi}_n(\bar{z}) = 0$ sein.

Dies zeigt die *Behauptung.*

Da $|\langle\!\langle \bar{\zeta} \rangle\!\rangle| = n$, ist n ein Teiler von $|\mathrm{U}(F_i)| = p^{[F_i:\mathbf{F}_p]} - 1$; cf. [**5,** Aufgabe 11.(1.c)]. Folglich ist $(p + (n))^{[F_i:\mathbf{F}_p]} = 1 + (n)$. Also ist $f = |\langle\!\langle p + (n) \rangle\!\rangle|$ ein Teiler von $[F_i : \mathbf{F}_p]$; cf. [**5,** Aufgabe 27.(1)]. Somit gibt es einen Zwischenkörper $F_i|F|\mathbf{F}_p$ mit $[F : \mathbf{F}_p] = f$; cf. [**5,** §2.5.4, Aufgabe 48.(2)]. Es ist $\mathrm{U}(F) \simeq \mathrm{C}_{p^f-1}$; cf. [**5,** Aufgabe 27.(5)]. Ist x ein Element von $\mathrm{U}(F)$ von Ordnung $p^f - 1 \equiv_n 0$ und ist $k \in [0, n-1]$ mit $\mathrm{ggT}(k, n) = 1$, dann hat $x^{k(p^f-1)/n}$ die Ordnung n ; cf. [**5,** Aufgabe 27.(2)]. Damit liegen in $\mathrm{U}(F)$ mindestens $\varphi(n)$ verschiedene Elemente von Ordnung n aus der Gruppe $\mathrm{U}(F_i)$. Jedes dieser Elemente ist gemäß obiger Behauptung eine Nullstelle von $\bar{\Phi}_n(X)$. Da auch $\deg(\bar{\Phi}_n(X)) \overset{\text{A. 17.(1)}}{=} \varphi(n)$ ist, zerfällt $\bar{\Phi}_n(X) \in F[X]$ in ein Produkt von Linearfaktoren. Somit liegen alle Nullstellen, die $\bar{\Phi}_n(X)$ in F_i hat, bereits in F. Es folgt $\bar{\zeta} \in F$ und somit $F_i = \mathbf{F}_p(\bar{\zeta}) \subseteq F \subseteq F_i$, i.e. $F_i = F$. Dann ist aber auch $[F_i : \mathbf{F}_p] = [F : \mathbf{F}_p] = f$.

Schließlich ist noch $df = \varphi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] \overset{\text{A. 43.(2)}}{=} \sum_{k\in[1,\tilde{d}]} e_k[F_k : \mathbf{F}_p] = \tilde{d}f$ und somit $d = \tilde{d}$. ▫

Beispiel 132 Sei $p \in \mathbf{Z}_{>0}$ prim. In $\mathbf{Z}[\zeta_{45}]$ wollen wir die Primidealfaktorzerlegungen von (p) ermitteln und mit der Aussage von Satz 131 vergleichen. Schreibe $\zeta := \zeta_{45}$. Es ist $\Phi_{45}(X) = X^{24} - X^{21} + X^{15} - X^{12} + X^9 - X^3 + 1$.

(1) Sei $p = 2$. Es ist $e = \varphi(1) = 1$. Es ist $f = |\langle\!\langle 2 + (45) \rangle\!\rangle| = 12$, da $2^{12} = 91 \cdot 45 + 1 \equiv_{45} 1$ und 12 der dafür kleinste Exponent $\geqslant 1$ ist. Desweiteren erhalten wir $d = \varphi(45)/12 = (3-1) \cdot 3 \cdot (5-1)/12 = 2$. In der Tat wird

$$\bar{\Phi}_{45}(X) \;=\; (X^{12} + X^3 + \bar{1})^1 (X^{12} + X^9 + \bar{1})^1 \;\in\; \mathbf{F}_2[X]$$

die Zerlegung in normierte irreduzible Faktoren und also

$$(2) \;=\; (\zeta^{12} + \zeta^3 + 1,\, 2)^1 (\zeta^{12} + \zeta^9 + \zeta,\, 2)^1$$

die Primidealfaktorzerlegung.

(2) Sei $p = 3$. Es ist $e = \varphi(9) = (3-1) \cdot 3 = 6$. Es ist $f = |\langle\!\langle 3 + (5) \rangle\!\rangle| = 4$, da $3^4 = 16 \cdot 5 + 1 \equiv_5 1$ und 4 der dafür kleinste Exponent $\geqslant 1$ ist. Es ist $d = \varphi(5)/4 = (5-1)/4 = 1$. In der Tat wird

$$\bar{\Phi}_{45}(X) \;=\; (X^4 + X^3 + X^2 + X + \bar{1})^6 \;\in\; \mathbf{F}_3[X]$$

die Zerlegung in normierte irreduzible Faktoren und also

$$(3) \;=\; (\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1,\, 3)^6$$

die Primidealfaktorzerlegung.

(3) Sei $p = 5$. Es ist $e = \varphi(5) = 5 - 1 = 4$. Es ist $f = |\langle\!\langle 5 + (9) \rangle\!\rangle| = 6$, da $5^6 = 1736 \cdot 9 + 1 \equiv_9 1$ und 6 der dafür kleinste Exponent $\geqslant 1$ ist. Es ist $d = \varphi(9)/6 = 3 \cdot (3-1)/6 = 1$. In der Tat wird

$$\bar{\Phi}_{45}(X) \;=\; (X^6 + X^3 + \bar{1})^4 \;\in\; \mathbf{F}_5[X]$$

die Zerlegung in normierte irreduzible Faktoren und also

$$(5) \;=\; (\zeta^6 + \zeta^3 + 1,\, 5)^4$$

die Primidealfaktorzerlegung.

(4) Sei $p = 11$. Es ist $e = \varphi(1) = 1$. Es ist $f = |\langle\!\langle 11 + (45) \rangle\!\rangle| = 6$, da sich $11^6 = 39368 \cdot 45 + 1 \equiv_{45} 1$ ergibt und 6 der dafür kleinste Exponent $\geqslant 1$ ist. Es ist $d = \varphi(45)/6 = (3-1) \cdot 3 \cdot (5-1)/6 = 4$. In der Tat wird

$$\bar{\Phi}_{45}(X) \;=\; (X^6 + \bar{3}X^3 + \bar{9})^1 (X^6 + \bar{4}X^3 + \bar{5})^1 (X^6 + \bar{5}X^3 + \bar{3})^1 (X^6 + \bar{9}X^3 + \bar{4})^1 \;\in\; \mathbf{F}_{11}[X]$$

und also

$$(11) \;=\; (\zeta^6 + 3\zeta^3 + 9,\, 11)^1 (\zeta^6 + 4\zeta^3 + 5,\, 11)^1 (\zeta^6 + 5\zeta^3 + 3,\, 11)^1 (\zeta^6 + 9\zeta^3 + 4,\, 11)^1$$

die Primidealfaktorzerlegung.

Beispiel 133 In $\mathbf{Z}[\zeta_{120}]$ wollen wir die Primidealfaktorzerlegung von (3) ermitteln und mit der Aussage von Satz 131 vergleichen. Schreibe $\zeta := \zeta_{120}$.

Es ist $\Phi_{120}(X) = X^{32} + X^{28} - X^{20} - X^{16} - X^{12} + X^4 + 1$.

Es ist $e = \varphi(3) = 3 - 1 = 2$. Es ist $f = |\langle\!\langle 3 + (40) \rangle\!\rangle| = 4$, da $3^4 = 2 \cdot 40 + 1 \equiv_{40} 1$ und 4 der dafür kleinste Exponent $\geqslant 1$ ist. Es ist $d = \varphi(40)/6 = (2-1) \cdot 4 \cdot (5-1)/4 = 4$. In der Tat wird

$$\bar{\Phi}_{120}(X) \;=\; (X^4 + X^2 + X + \bar{1})^2 (X^4 + X^2 - X + \bar{1})^2 (X^4 + X^3 + X^2 + \bar{1})^2 (X^4 - X^3 + X^2 + \bar{1})^2 \;\in\; \mathbf{F}_3[X]$$

die Zerlegung in normierte irreduzible Faktoren und also

$$(3) \;=\; (\zeta^4 + \zeta^2 + \zeta + 1,\, 3)^2 (\zeta^4 + \zeta^2 - \zeta + 1,\, 3)^2 (\zeta^4 + \zeta^3 + \zeta^2 + 1,\, 3)^2 (\zeta^4 - \zeta^3 + \zeta^2 + 1,\, 3)^2$$

die Primidealfaktorzerlegung.

4.2 Verzweigungsindex und Trägheitsgrad

4.2.1 Allgemeinfall

Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt. Sei $L|K$ eine endliche Körpererweiterung. Schreibe $\ell := [L : K]$. Sei $B := \Gamma_L(A)$.

Definition 134 Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$. Betrachte die Primidealfaktorzerlegung

$$B\mathfrak{p} \;=\; \prod_{i\in[1,d]} \mathfrak{q}_i^{e_i} \;,$$

wobei $d \geqslant 1$, wobei $\mathfrak{q}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ und $e_i \geqslant 1$ für $i \in [1,d\,]$ und wobei $\mathfrak{q}_i \neq \mathfrak{q}_j$ für $i,\, j \in [1,d\,]$ mit $i \neq j$; cf. Satz 63.

Für $i \in [1,d\,]$ ist $A/\mathfrak{p} \longrightarrow\!\!\!\!\!\rightarrow B/\mathfrak{q}_i\,,\; a+\mathfrak{p} \longmapsto\!\!\!\!\!\rightarrow a+\mathfrak{q}_i$ ein injektiver Körpermorphismus, desvermöge $(B/\mathfrak{q}_i)|(A/\mathfrak{p})$ eine endliche Körpererweiterung wird; cf. Aufgabe 43.(1). Sei $f_i := [\,B/\mathfrak{q}_i \,:\, A/\mathfrak{p}\,]$.

Folgende Zerlegungsparameter bezüglich $L|K$ über A sind hierbei aufgetreten.

Es heißt d die *Zerlegungsbreite* von $\mathfrak{p}$.

Es heißt e_i der *Verzweigungsindex* von $\mathfrak{q}_i$ für $i \in [1,d\,]$.

Es heißt f_i der *Trägheitsgrad* von $\mathfrak{q}_i$ für $i \in [1,d\,]$.

Dabei ist $\sum_{i\in[1,d]} e_i f_i = \ell$; cf. Aufgabe 43.(2).

Beispiel 135

(1) Sei $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt[3]{2})$. Schreibe $\delta := \sqrt[3]{2}$. Es ist $B = \mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$; cf. Aufgabe 19.(2). Es ist

$$\mu_{\delta,\mathbf{Q}}(X) \;\overset{\text{A. 7.(1)}}{=}\; X^3-2 \;\equiv_5\; (X+2)^1(X^2-2X-1)^1$$

die Zerlegung in normierte irreduzible Faktoren. Wie in der Lösung zu Aufgabe 30.(2) erklärt, wird die Primidealfaktorzerlegung in $\mathbf{Z}[\delta]$ somit

$$\begin{array}{rcl}(5) & = & (\delta+2,\,5)^1 \cdot (\delta^2-2\delta-1,\,5)^1 \\ & = & (\delta^2+1)^1 \cdot (\delta^2-2\delta-1)^1\end{array}$$

Die Zerlegungsbreite von (5) ist $d = 2$.

Das Primideal $\mathfrak{q}_1 := (\delta+2,\,5)$ hat Verzweigungsindex $e_1 = 1$ und Trägheitsgrad $f_1 = \deg(X+2) = 1$; cf. Lösung zu Aufgabe 30.(2).

Das Primideal $\mathfrak{q}_2 := (\delta^2-2\delta-1,\,5)$ hat Verzweigungsindex $e_2 = 1$ und Trägheitsgrad $f_2 = \deg(X^2-2X-1) = 2$; cf. Lösung zu Aufgabe 30.(2).

(2) Satz 131 und Beispiele 132 und 133 erläutern die Zerlegungsparameter im Kreisteilungsringfall.

Lemma 136 (Verzweigung nur bei Diskriminantenteilern, monogener Fall)

Wir setzen voraus, daß wir ein $b \in B$ haben mit $B = A[b]$.

Wir schreiben $\underline{g} := (\,b^i \,:\, i \in [0,\ell-1]\,)$.

Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$ *gegeben.*

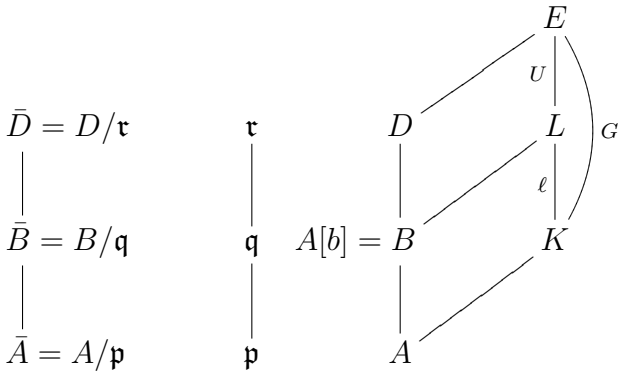
Sei $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ *mit* $\mathfrak{q} \cap A = \mathfrak{p}$ *gegeben; cf. Aufgaben* 29.(1) *und* 43.(1).

Ist $\Delta_{L|K,\underline{g}} \not\equiv_{\mathfrak{p}} 0$*, dann ist der Verzweigungsindex von* $\mathfrak{q}$ *gleich* 1.

Beweis. Schreibe $\bar{A} := A/\mathfrak{p}$ und $\bar{B} := B/\mathfrak{q}$. Sei $\bar{\mu}_{b,K}(X)$ das Bild von $\mu_{b,K}(X)$ in $\bar{A}$ unter der koeffizientenweise angewandten Restklassenabbildung $A \longrightarrow\!\!\!\!\!\rightarrow \bar{A}$. Gemäß Lösung zu Aufgabe 30.(2) haben wir zu zeigen, daß $\bar{\mu}_{b,K}(X)$ in $\bar{A}[X]$ in ein Produkt paarweiser verschiedener normierter irreduzibler Faktoren zerfällt.

Sei E ein Zerfällungskörper von $L|K$. Sei $D := \Gamma_E(A)$. Trete $\mathfrak{r} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ in der Primidealfaktorisierung von $\mathfrak{q}D$ auf, i.e. sei $\mathfrak{q} = B \cap \mathfrak{r}$. Schreibe $\bar{D} := D/\mathfrak{r}$. Es sind $\bar{D}|\bar{B}|\bar{A}$ endliche Körpererweiterungen. Cf. Aufgaben 29.(1) und 43.(1).

Sei $U := \mathrm{Gal}(E|L) \leqslant \mathrm{Gal}(E|K) =: G$. Sei $G = \bigsqcup_{j\in[1,\ell]} \tau_j U$ mit $\tau_j \in G$ für $j \in [1,\ell]$.



Es ist $\Delta_{L|K,\underline{g}} = \prod_{1\leqslant i<j\leqslant \ell}(\tau_j(b) - \tau_i(b))^2$; cf. Bemerkung 25.

Da $\Delta_{L|K,\underline{g}} \notin \mathfrak{p} = A \cap \mathfrak{r}$, folgt $\Delta_{L|K,\underline{g}} \notin \mathfrak{r}$ und also $\tau_j(b) \not\equiv_{\mathfrak{r}} \tau_i(b)$ für $1 \leqslant i < j \leqslant \ell$.

Es liegt in $D[X]$ die Zerlegung

$$\mu_{b,K}(X) \overset{\text{L. 14, L 20.(1)}}{=} \prod_{i\in[1,\ell]} (X - \tau_i(b)) \ ,$$

vor, welche in $\bar{D}[X]$ zu

$$\bar{\mu}_{b,K}(X) \ = \ \prod_{i\in[1,\ell]} (X - (\tau_i(b) + \mathfrak{r}))$$

wird. Nach vorigem ist dies ein Produkt paarweise verschiedener Linearfaktoren. Somit kann $\bar{\mu}_{b,K}(X)$ auch in seiner Zerlegung in normierte irreduzible Faktoren in $\bar{A}[X]$ keinen normierten irreduziblen Faktor mit Exponent $\geqslant 2$ aufweisen. ▫

Beispiel.

(1) Wir setzen Beispiel 135.(1) fort, in welchem wir $\mathbf{Q}(\delta)|\mathbf{Q}$ mit $\delta = \sqrt[3]{2}$ betrachtet haben. Es war $\mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$.

Es ist $\Delta_{\mathbf{Q}(\delta)} = -2^2 \cdot 3^3$; cf. Aufgabe 19.(2). Es ist also 5 kein Teiler von $\Delta_{\mathbf{Q}(\delta)}$. Gemäß Lemma 136 sind die Verzweigungsindizes der Primideale von $\mathbf{Z}[\delta]$, die (5) enthalten, alle gleich 1.

Dies steht in Übereinstimmung mit der Primidealfaktorzerlegung aus loc. cit., viz. $(5) = (\delta^2+1)^1 \cdot (\delta^2 - 2\delta - 1)^1$.

(2) Ist $n \in \mathbf{Z}_{\geqslant 1}$ mit $\mathrm{v}_2(n) \neq 1$ gegeben, dann ist die Menge der Primteiler von n gleich der Menge der Primteiler von $\Delta_{\mathbf{Q}(\zeta_n)}$. Gemäß Lemma 136 hat ein Primideal von $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$, das eine Primzahl p enthält, die n nicht teilt, den Verzweigungsindex 1; cf. Satz 130.(1).

Da diesenfalls $\varphi(n[p]) = 1$ ist, steht dies in Übereinstimmung mit Satz 131.

4.2.2 Galoisfall

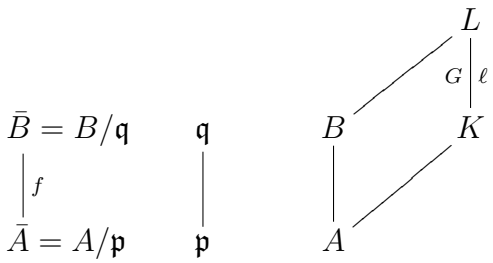
Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt. Sei $L|K$ eine endliche, galoische Körpererweiterung. Schreibe $G := \mathrm{Gal}(L|K)$ und $\ell := [L:K] = |G|$. Sei $B := \Gamma_L(A)$.

Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$. Sei $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ mit $\mathfrak{p} \subseteq \mathfrak{q}$; cf. Satz 63, Aufgabe 29.(1).

Schreibe $\bar{A} := A/\mathfrak{p}$. Sei $\bar{A}$ perfekt. Schreibe $\bar{B} := B/\mathfrak{q}$. Schreibe zuweilen $\bar{b} := b + \mathfrak{q}$ für $b \in B$.

Es ist $\mathfrak{p} = A \cap \mathfrak{q}$ und $\bar{B}|\bar{A}$ eine endliche Körpererweiterung; cf. Aufgabe 43.(1). Schreibe

$$\begin{aligned} e &:= \mathrm{v}_{\mathfrak{q}}(B\mathfrak{p}) \\ f &:= [\bar{B} : \bar{A}] \,. \end{aligned}$$



Definition 137

(1) Sei $G_{\mathfrak{q}} := \{\, \sigma \in G \,:\, \sigma(\mathfrak{q}) = \mathfrak{q} \,\}$ die *Zerlegungsgruppe* von $\mathfrak{q}$ für $L|K$.
Sei $L_{\mathrm{dec}} = L_{\mathrm{dec},\mathfrak{q}} := \mathrm{Fix}_{G_{\mathfrak{q}}}(L)$ der *Zerlegungskörper* von $\mathfrak{q}$ für $L|K$.

(2) Sei $I_{\mathfrak{q}} := \{\, \sigma \in G_{\mathfrak{q}} \,:\, \sigma(b) \equiv_{\mathfrak{q}} b \text{ für } b \in B \,\}$ die *Trägheitsgruppe* von $\mathfrak{q}$ für $L|K$.
Sei $L_{\mathrm{inert}} = L_{\mathrm{inert},\mathfrak{q}} := \mathrm{Fix}_{I_{\mathfrak{q}}}(L)$ der *Trägheitskörper* von $\mathfrak{q}$ für $L|K$.

Unten in Satz 143 werden wir sehen, daß Zerlegung nur unterhalb des Zerlegungskörpers stattfindet und Trägheit nur zwischen Zerlegungs- und Trägheitskörper. Daher die Namen; Trägheit ist engl. inertia, Zerlegung ist engl. decomposition.

Es ist $I_{\mathfrak{q}}$ der Kern der Abbildung $G_{\mathfrak{q}} \longrightarrow \mathrm{Aut}(\bar{B}|\bar{A})$, $\sigma \longmapsto (b+\mathfrak{q} \longmapsto \sigma(b)+\mathfrak{q})$, was wegen $\sigma(\mathfrak{q}) = \mathfrak{q}$ für $\sigma \in G_{\mathfrak{q}}$ ein wohldefinierter Gruppenmorphismus ist. Also ist

$$1 \leqslant I_{\mathfrak{q}} \trianglelefteq G_{\mathfrak{q}} \leqslant G \, .$$

Schreibe $B_{\mathrm{dec}} = B_{\mathrm{dec},\mathfrak{q}} := \Gamma_{L_{\mathrm{dec}}}(A) = B \cap L_{\mathrm{dec}}$ und $B_{\mathrm{inert}} = B_{\mathrm{inert},\mathfrak{q}} := \Gamma_{L_{\mathrm{inert}}}(A) = B \cap L_{\mathrm{inert}}$.

Schreibe $\mathfrak{q}_{\mathrm{dec}} := \mathfrak{q} \cap B_{\mathrm{dec}}$ und $\mathfrak{q}_{\mathrm{inert}} := \mathfrak{q} \cap B_{\mathrm{inert}}$.

Schreibe $\bar{B}_{\mathrm{dec}} := B_{\mathrm{dec}}/\mathfrak{q}_{\mathrm{dec}}$. Schreibe $\bar{B}_{\mathrm{inert}} := B_{\mathrm{inert}}/\mathfrak{q}_{\mathrm{inert}}$.

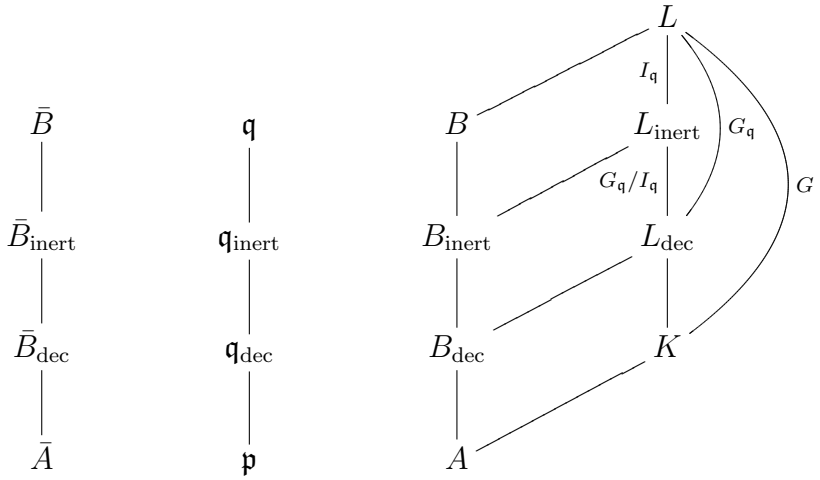
Wir erhalten die Körpererweiterungen $\bar{B}|\bar{B}_{\mathrm{inert}}|\bar{B}_{\mathrm{dec}}|\bar{A}$ nach Identifikation entlang der Bilder der injektiven Körpermorphismen

$$A/\mathfrak{p} \longrightarrow B_{\mathrm{dec}}/\mathfrak{q}_{\mathrm{dec}} \longrightarrow B_{\mathrm{inert}}/\mathfrak{q}_{\mathrm{inert}} \longrightarrow B/\mathfrak{q} \, ,$$

die jeweils die Restklasse eines Elements auf die Restklasse desselben Elements, modulo dem größeren Ideal, abbilden; cf. Aufgabe 43.(1).

> Die Bezeichnungen $\bar{B}_{\mathrm{inert}}$ und $\bar{B}_{\mathrm{dec}}$ werden nur im Verlauf des Beweises von Satz 143 benötigt. Cf. loc. cit. $(1,3)$ unten.

Wir befinden uns also in folgender Situation.



Lemma 138 (Galoisbahn von Primidealen) *Betrachte die Primidealfaktorzerlegung*

$$B\mathfrak{p} \;=\; \prod_{i \in [1,d]} \mathfrak{q}_i^{e_i} \, ,$$

wobei $d \geqslant 1$, *wobei* $\mathfrak{q}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ *für* $i \in [1,d]$ *mit o.E.* $\mathfrak{q} = \mathfrak{q}_1$, *wobei* $e_i \geqslant 1$ *für* $i \in [1,d]$ *mit* $e := e_1$ *und wobei* $\mathfrak{q}_i \neq \mathfrak{q}_j$ *für* $i, j \in [1,d]$ *mit* $i \neq j$ *; cf. Satz* 63, *Aufgabe* 29.(1). *Schreibe* $f_i := [B/\mathfrak{q}_i : A/\mathfrak{p}]$ *für* $i \in [1,d]$ *und* $f := f_1$.

(1) *Es ist* $\{\, \mathfrak{q}_i \,:\, i \in [1,d] \,\} = \{\, \sigma(\mathfrak{q}) \,:\, \sigma \in G \,\}$.

(2) *Es ist* $e = e_i$ *für* $i \in [1,d]$.
Wir nennen dann e *auch den* Verzweigungsindex *von* $\mathfrak{p}$ *für* $L|K$.

(3) *Es ist* $f = f_i$ *für* $i \in [1,d]$.
Wir nennen dann f *auch den* Trägheitsgrad *von* $\mathfrak{p}$ *für* $L|K$.

(4) *Es ist* $d\,e\,f = \ell$.
Es ist $d = |G|/|G_{\mathfrak{q}}| = [L_{\mathrm{dec}} : L]$ *und also* $|G_{\mathfrak{q}}| = e\,f$.
Seien $\rho_i \in G$ *für* $i \in [1,d]$ *so gewählt, daß* $G = \bigsqcup_{i\in[1,d]} \rho_i\, G_{\mathfrak{q}}$ *ist.*
Dann haben wir haben die Primidealfaktorzerlegung

$$B\mathfrak{p} \;=\; \prod_{i\in[1,d]} \rho_i(\mathfrak{q})^e \;.$$

Beweis.

Ad (1). Zu $\overset{!}{\supseteq}$. Wir haben zu zeigen, daß für $\sigma \in G$ auch $\sigma(\mathfrak{q})$ in der Primidealfaktorzerlegung von $B\mathfrak{p}$ auftritt, mit Aufgabe 29.(1) also, daß $B\mathfrak{p} \subseteq \sigma(\mathfrak{q})$ liegt, i.e. daß $\mathfrak{p} \subseteq \sigma(\mathfrak{q})$ liegt. Aber aus $\mathfrak{p} \subseteq \mathfrak{q}$ folgt $\mathfrak{p} = \sigma(\mathfrak{p}) \subseteq \sigma(\mathfrak{q})$.

Zu $\overset{!}{\subseteq}$. *Annahme,* nicht. Dann gibt es ein $j \in [2,d]$ so, daß $\mathfrak{q}_j \neq \sigma(\mathfrak{q})$ ist für alle $\sigma \in G$.

Nach Umnumerieren der Primideale können wir von

$$\{\,\sigma(\mathfrak{q}) \,:\, \sigma \in G\,\} \;=\; \{\,\mathfrak{q}_i \,:\, i \in [1,j-1]\,\}\;.$$

ausgehen. Es ist $B \longrightarrow \prod_{i\in[1,j]} B/\mathfrak{q}_i\,,\ b \longmapsto (b+\mathfrak{q}_i)_{i\in[1,j]}$ surjektiv; cf. Aufgabe 26.(2). Insbesondere können wir ein $b \in B$ mit $b \equiv_{\mathfrak{q}_i} 1$ für $i \in [1,j-1]$ und mit $b \equiv_{\mathfrak{q}_j} 0$ wählen.

Damit ist $b \notin \sigma^{-1}(\mathfrak{q})$ und also $\sigma(b) \notin \mathfrak{q}$ für $\sigma \in G$. Es folgt

$$\mathrm{N}_{L|K}(b) \overset{\text{K. 16}}{=} \prod_{\sigma\in G} \underbrace{\sigma(b)}_{\notin \mathfrak{q}} \;\notin\; \mathfrak{q}\;.$$

Aber es ist $b \in \mathfrak{q}_j$ und also auch

$$\mathrm{N}_{L|K}(b) \overset{\text{K. 16}}{=} b \cdot \prod_{\sigma\in G\smallsetminus\{\mathrm{id}_L\}} \sigma(b) \overset{\text{L. 20.(1, 3)}}{\in} \mathfrak{q}_j \cap A \underset{\text{A. 43.(1)}}{\overset{\text{A. 29.(1)}}{=}} \mathfrak{p} \;\subseteq\; \mathfrak{q}\;.$$

Wir haben einen *Widerspruch.*

Ad (2). Sei $j \in [1,d]$. Sei $\sigma_j \in G$ mit $\sigma_j(\mathfrak{q}) = \mathfrak{q}_j$ gewählt; cf. (1). Es wird

$$\prod_{i\in[1,d]} \mathfrak{q}_i^{e_i} \;=\; B\mathfrak{p} \;=\; \sigma_j(B\mathfrak{p}) \;=\; \sigma_j\Big(\prod_{i\in[1,d]} \mathfrak{q}_i^{e_i}\Big) \;=\; \prod_{i\in[1,d]} \sigma_j(\mathfrak{q}_i)^{e_i}\;.$$

Da die Primideale $\mathfrak{q}_i$ für $i \in [1,d]$ paarweise verschieden sind, gilt dies auch für die Primideale $\sigma_j(\mathfrak{q}_i)$ für $i \in [1,d]$. Da $\sigma_j(\mathfrak{q}_1) = \mathfrak{q}_j$ ist, folgt also

$$e_j \;=\; \mathrm{v}_{\mathfrak{q}_j}(B\mathfrak{p}) \;=\; \mathrm{v}_{\sigma_j(\mathfrak{q}_1)}(B\mathfrak{p}) \;=\; e_1 \;=\; e\,;$$

cf. Lemma 65.

Ad (3). Seien $\sigma_j \in G$ für $j \in [1,d]$ wie in (2) gewählt.

Wir haben $\bar{A}$-lineare Körpermorphismen

$$\begin{array}{rcl} \bar{B} \;=\; B/\mathfrak{q} & \longleftrightarrow & B/\mathfrak{q}_j \\ b+\mathfrak{q} & \longmapsto & \sigma_j(b)+\mathfrak{q}_j \\ \sigma_j^{-1}(b)+\mathfrak{q} & \longleftarrow\!\shortmid & b+\mathfrak{q}_j\;, \end{array}$$

wohldefiniert in beide Richtungen, da $\sigma_j(\mathfrak{q}) = \mathfrak{q}_j$ und also auch $\mathfrak{q} = \sigma_j^{-1}(\mathfrak{q}_j)$ ist; nach Konstruktion liegen dann in beiden Richtungen Körpermorphismen vor, die sich gegenseitig invertieren. Folglich ist $[\bar{B} : \bar{A}] = [B/\mathfrak{q} : A/\mathfrak{p}] = [B/\mathfrak{q}_j : A/\mathfrak{p}]$.

Ad (4). Sei $G = \bigsqcup_{i\in[1,\tilde{d}]} \rho_i\, G_{\mathfrak{q}}$, wobei $\rho_i \in G$ liege für $i \in [1,\tilde{d}]$. Dann ist

$$\{\,\rho_i(\mathfrak{q}) \,:\, i \in [1,\tilde{d}]\,\} \;=\; \{\,\sigma(\mathfrak{q}) \,:\, \sigma \in G\,\} \;\overset{(1)}{=}\; \{\,\mathfrak{q}_i \,:\, i \in [1,d]\,\}\;,$$

denn für gegebenes $\sigma \in G$ können wir ein $i \in [1,\tilde{d}]$ und ein $\tau \in G_{\mathfrak{q}}$ mit $\sigma = \rho_i \circ \tau$ finden, was $\sigma(\mathfrak{q}) = (\rho_i \circ \tau)(\mathfrak{q}) = \rho_i(\mathfrak{q})$ nach sich zieht.

Sind $i,\, j \in [1,\tilde{d}]$ gegeben mit $i \neq j$, dann ist $\rho_i(\mathfrak{q}) \neq \rho_j(\mathfrak{q})$, denn *wäre* $\rho_i(\mathfrak{q}) = \rho_j(\mathfrak{q})$, dann wäre $(\rho_j^{-1} \circ \rho_i)(\mathfrak{q}) = \mathfrak{q}$, also $\rho_j^{-1} \circ \rho_i \in G_{\mathfrak{q}}$, mithin $\rho_i\, G_{\mathfrak{q}} = \rho_j\, G_{\mathfrak{q}}$, was *nicht* der Fall ist.

> Man kann hierzu auch das Bahnenlemma heranziehen; cf. **[6,** Lemma 5].

Es folgt $d = \tilde{d}$ und, dank (2), auch $B\mathfrak{p} = \prod_{i\in[1,d]} \rho_i(\mathfrak{q})^e$.

Es folgt $d = |G|/|G_{\mathfrak{q}}| = [L_{\mathrm{dec}} : K]$.

Die Gleichung $d\,e\,f = \ell$ folgt aus $(2,3)$ und aus Aufgabe 43.(2). ▫

Beispiel 139

Sei $n \geqslant 1$, $\mathrm{v}_2(n) \neq 1$, $A = \mathbf{Z}$, $K = \mathbf{Q}$ und $L = \mathbf{Q}(\zeta_n)$. Dann ist $B = \mathbf{Z}[\zeta_n]$; cf. Satz 130.(1). Ferner ist $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ galoisch; cf. Aufgabe 17.(1).

Sei $p \in \mathbf{Z}_{>0}$ prim. Sei $(p) = \prod_{i\in[1,d]} \mathfrak{q}_i^{e_i}$, wobei $d \geqslant 1$, wobei $\mathfrak{p}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ und $e_i \geqslant 1$ für $i \in [1,d]$ und wobei $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i,\, j \in [1,n]$ mit $i \neq j$; cf. Satz 63.

Gemäß Lemma 138.(2) ist e_i konstant in i. Gemäß Satz 131 gilt hier genauer $e_i = \varphi(n[p])$, unabhängig von i.

Gemäß Lemma 138.(3) ist $f_i := [\mathbf{Z}[\zeta_n]/\mathfrak{q}_i : \mathbf{Z}/(p)]$ konstant in i. Gemäß Satz 131 gilt hier genauer $f_i = |\langle\!\langle p + (n/n[p])\rangle\!\rangle|$, unabhängig von i.

Lemma 140

(1) *Es ist* $B\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}^e$ *und* $\mathrm{v}_{\mathfrak{q}_{\mathrm{dec}}}(B_{\mathrm{dec}}\mathfrak{p}) = 1$.

(2) *Es ist* $[\bar{B}_{\mathrm{dec}} : \bar{A}] = 1$, *i.e. es ist* $A/\mathfrak{p} \xrightarrow{\sim} B_{\mathrm{dec}}/\mathfrak{q}_{\mathrm{dec}}$, $a + \mathfrak{p} \longmapsto a + \mathfrak{q}_{\mathrm{dec}}$, *i.e. es ist* $\bar{A} = \bar{B}_{\mathrm{dec}}$ *(nach Identifikation).*

Beweis. Wir wollen zeigen, daß $\mathfrak{q}$ das einzige Primideal von B ist, das $B\mathfrak{q}_{\mathrm{dec}}$ enthält. Sei dazu $\tilde{\mathfrak{q}} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ mit $B\mathfrak{q}_{\mathrm{dec}} \subseteq \tilde{\mathfrak{q}}$ gegeben. Für ein $\sigma \in \mathrm{Gal}(L|L_{\mathrm{dec}}) = G_{\mathfrak{q}}$ wird dann $\tilde{\mathfrak{q}} = \sigma(\mathfrak{q}) = \mathfrak{q}$; cf. Lemma 138.(1).

Somit ist $B\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}^{e'}$ für ein $e' \geqslant 1$; cf. Aufgabe 29.(1). Schreibe $f' := [\bar{B} : \bar{B}_{\mathrm{dec}}]$. Es wird $e'f' = [L : L_{\mathrm{dec}}]$; cf. Lemma 138.(4).

Schreibe $B_{\mathrm{dec}}\mathfrak{p} = \mathfrak{q}_{\mathrm{dec}}^{e''}\mathfrak{x}$ für ein $\mathfrak{x} \in \mathrm{Ideale}^{\times}(B_{\mathrm{dec}})$ mit $\mathfrak{q}_{\mathrm{dec}} + \mathfrak{x} = (1)$; cf. Satz 63, Aufgabe 29.(4). Es ist $e'' = \mathrm{v}_{\mathfrak{q}_{\mathrm{dec}}}(B_{\mathrm{dec}}\mathfrak{p})$. Ferner ist $B\mathfrak{p} = (B\mathfrak{q}_{\mathrm{dec}})^{e''}(B\mathfrak{x}) = \mathfrak{q}^{e'e''}(B\mathfrak{x})$ mit $(1) = B\mathfrak{q}_{\mathrm{dec}} + B\mathfrak{x} = \mathfrak{q}^{e'} + B\mathfrak{x}$ und folglich auch $\mathfrak{q} + B\mathfrak{x} = (1)$; cf. Aufgabe 29.(4). Somit ist $e = \mathrm{v}_{\mathfrak{q}}(B\mathfrak{p}) = e'e''$.

Schreibe $f'' := [\bar{B}_{\mathrm{dec}} : \bar{A}]$. Es ist $f'f'' = f$; cf. [**5,** §2.2].

Es ist $d \overset{\text{L. 138.(4)}}{=} [L_{\mathrm{dec}} : K]$. Es folgt

$$e'f' \;=\; [L : L_{\mathrm{dec}}] \;=\; [L : K]/d \overset{\text{L. 138.(4)}}{=} d\,ef/d \;=\; ef \;=\; e'e''f'f'' \,.$$

Somit ist $e'' = 1$, $f'' = 1$ und also $e' = e$, $f' = f$.

Mithin ergibt sich $B\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}^{e'} = \mathfrak{q}^e$ und $\mathrm{v}_{\mathfrak{q}_{\mathrm{dec}}}(B_{\mathrm{dec}}\mathfrak{p}) = e'' = 1$ und $[\bar{B}_{\mathrm{dec}} : \bar{A}] = f'' = 1$. ▫

Lemma 141

(1) *Die Körpererweiterung* $\bar{B}|\bar{A}$ *ist galoisch.*

(2) *Wir haben einen Gruppenisomorphismus*

$$\begin{array}{rcl} G_{\mathfrak{q}}/I_{\mathfrak{q}} & \xrightarrow{\sim} & \mathrm{Gal}(\bar{B}|\bar{A}) \\ \sigma I_{\mathfrak{q}} & \longmapsto & (\bar{\sigma} : \bar{b} \longmapsto \bar{\sigma}(\bar{b}) := \overline{\sigma(b)}) \,. \end{array}$$

(3) *Es ist* $|I_{\mathfrak{q}}| = [L : L_{\mathrm{inert}}] = e$ *und* $|G_{\mathfrak{q}}/I_{\mathfrak{q}}| = [L_{\mathrm{inert}} : L_{\mathrm{dec}}] = f$.

Beweis. Da (nach Identifikation) $\bar{A} = \bar{B}_{\mathrm{dec}}$ ist und da die Verzweigungsindizes von $\mathfrak{p}$ und von $\mathfrak{q}_{\mathrm{dec}}$ beide gleich e sind, dürfen wir $K = L_{\mathrm{dec}}$, $\mathfrak{p} = \mathfrak{q}_{\mathrm{dec}}$ und $G = G_{\mathfrak{q}}$ annehmen; cf. Lemma 140.(1, 2).

Sei $x \in B$ mit $\bar{B} = \bar{A}(\bar{x})$ gewählt, was wegen $\bar{A}$ perfekt möglich ist; cf. [**5,** Aufgabe 54]. Es zerfällt $\mu_{x,K}(X)$ in $L[X]$ in ein Produkt von Linearfaktoren; cf. Lemma 14. Es ist $\mu_{x,K}(X) \in A[X]$ und zerfällt in $B[X]$ in ein Produkt von Linearfaktoren; cf. Aufgabe 2.(8).

Also können wir das Bild $\bar{\mu}_{x,K}(X) \in \bar{A}[X]$ unter der koeffizientenweise angewandten Restklassenabbildung bilden, und dieses zerfällt in $\bar{B}[X]$ in ein Produkt von Linearfaktoren. Es ist $\bar{\mu}_{x,K}(\bar{x}) = 0$. Also ist $\mu_{\bar{x},\bar{A}}(X)$ ein Teiler von $\bar{\mu}_{x,K}(X)$; cf. [**5,** §2.3.2]. Somit zerfällt auch $\mu_{\bar{x},\bar{A}}(X) \in \bar{B}[X]$ in ein Produkt von Linearfaktoren. Da $\bar{x}$ eine Nullstelle von $\mu_{\bar{x},\bar{A}}(X)$ ist und bereits $\bar{B} = \bar{A}(\bar{x})$ gilt, ist $\bar{B}$ Zerfällungskörper von $\mu_{\bar{x},\bar{A}}(X) \in \bar{A}[X]$; cf. [**5,** §2.5.1]. Da zudem $\bar{A}$ perfekt ist, ist $\bar{B}|\bar{A}$ mithin galoisch; cf. [**5,** §3.5.1.4]. Dies zeigt (1).

Die Abbildung $G \longrightarrow \mathrm{Gal}(\bar{B}|\bar{A}), \sigma \longmapsto \bar{\sigma}$ ist ein Gruppenmorphismus, da sich für $\sigma,\ \rho \in G$ für $b \in B$

$$\bar{\sigma}(\bar{\rho}(\bar{b})) \ = \ \bar{\sigma}(\overline{\rho(b)}) \ = \ \overline{\sigma(\rho(b))} \ = \ \overline{(\sigma \circ \rho)(b)} \ = \ \overline{(\sigma \circ \rho)}(\bar{b})$$

ergibt und somit $\bar{\sigma} \circ \bar{\rho} = \overline{\sigma \circ \rho}$.

Sei $\tau \in \mathrm{Gal}(\bar{B}|\bar{A})$ gegeben. Es ist $\tau(\bar{x})$ eine Nullstelle von $\mu_{\bar{x},\bar{A}}(X)$ und damit auch eine Nullstelle von $\bar{\mu}_{x,K}(X)$. Da $\mu_{x,K}(X)$ in $B[X]$ in Linearfaktoren zerfällt, gibt es also ein $y \in B$ mit $\mu_{x,K}(y) = 0$ und $\bar{y} = \tau(\bar{x})$.

Wähle $\sigma \in G$ mit $\sigma(x) = y$; cf. [**5,** §2.3.4]. Dann ist $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)} = \bar{y} = \tau(\bar{x})$. Da $\bar{B} = \bar{A}(\bar{x})$ ist, folgt $\bar{\sigma} = \tau$.

Ferner ist der Kern von $\sigma \longmapsto \bar{\sigma}$ gegeben durch

$$\{\, \sigma \in G \,:\, \bar{\sigma} = \mathrm{id}_{\bar{B}} \,\} \ = \ \{\, \sigma \in G \,:\, \sigma(b) \equiv_{\mathfrak{q}} b \text{ für } b \in B \,\} \ = \ I_{\mathfrak{q}} \ .$$

Damit ist auch (2) gezeigt.

Insbesondere ist $|G/I_{\mathfrak{q}}| = |\mathrm{Gal}(\bar{B}|\bar{A})| = [\bar{B} : \bar{A}] = f$. Da dank Lemma 138.(4) sich $|G| = ef$ ergibt, folgt hieraus auch $|I_{\mathfrak{q}}| = e$. ▫

Lemma 142

(1) *Es ist* $B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}_{\mathrm{inert}}$. *Es ist* $[\bar{B}_{\mathrm{inert}} : \bar{B}_{\mathrm{dec}}] = f$.

(2) *Es ist* $B\mathfrak{q}_{\mathrm{inert}} = \mathfrak{q}^e$.
Es ist $[\bar{B} : \bar{B}_{\mathrm{inert}}] = 1$, *i.e. es ist* $B_{\mathrm{inert}}/\mathfrak{q}_{\mathrm{inert}} \xrightarrow{\sim} B/\mathfrak{q}$, $x + \mathfrak{q}_{\mathrm{inert}} \longmapsto x + \mathfrak{q}$, *i.e. es ist* $\bar{B}_{\mathrm{inert}} = \bar{B}$ *(nach Identifikation).*

Beweis. Da $\mathfrak{q}$ dank Lemma 140.(1) das einzige Primideal von B ist, das $\mathfrak{q}_{\mathrm{dec}}$ enthält, ist auch $\mathfrak{q}$ das einzige Primideal von B, das $\mathfrak{q}_{\mathrm{inert}}$ enthält, und es ist $\mathfrak{q}_{\mathrm{inert}}$ das einzige Primideal von B_{inert} , das $\mathfrak{q}_{\mathrm{dec}}$ enthält. Letzteres deswegen, da die *Annahme*, es gäbe ein $\mathfrak{r} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B_{\mathrm{inert}})$ mit $\mathfrak{r} \neq \mathfrak{q}_{\mathrm{inert}}$ und $\mathfrak{r} \supseteq \mathfrak{q}_{\mathrm{dec}}$ dazu führte, daß wir in der Primidealfaktorzerlegung von $B\mathfrak{r}$ einen Faktor $\mathfrak{s} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ wählen könnten, der dann auch $\mathfrak{s} \supseteq \mathfrak{r}$ erfüllte, woraus man dank Aufgabe 43.(1) auf $\mathfrak{s} \cap B_{\mathrm{inert}} = \mathfrak{r}$ schließen könnte, also auf $\mathfrak{s} \neq \mathfrak{q}$, und auch auf $\mathfrak{s} \cap B_{\mathrm{dec}} = \mathfrak{q}_{\mathrm{dec}}$, was aber *nicht* geht. Die Zerlegungsbreiten von $\mathfrak{q}_{\mathrm{dec}}$ für $L_{\mathrm{inert}}|L_{\mathrm{dec}}$ und von $\mathfrak{q}_{\mathrm{inert}}$ für $L|L_{\mathrm{inert}}$ sind also beide gleich 1.

Ad (2). Wenden wir Lemma 141.(2) auf $L|L_{\mathrm{inert}}$ und $\mathfrak{q}_{\mathrm{inert}} \subseteq \mathfrak{q}$ an, so folgt aus der Tatsache, daß $G_{\mathfrak{q}} \cap I_{\mathfrak{q}} = I_{\mathfrak{q}}$ die Zerlegungsgruppe von $\mathfrak{q}$ über L_{inert} sowie $I_{\mathfrak{q}} \cap I_{\mathfrak{q}} = I_{\mathfrak{q}}$ die Trägheitsgruppe von $\mathfrak{q}$ über L_{inert} ist, daß $|\mathrm{Gal}(\bar{B}|\bar{B}_{\mathrm{inert}})| = 1$ ist. Also ist auch $[\bar{B} : \bar{B}_{\mathrm{inert}}] = 1$. Da $[L : L_{\mathrm{inert}}] = |I_{\mathfrak{q}}| = e$ ist nach Lemma 141.(3), folgt $B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}^e_{\mathrm{inert}}$; cf. Aufgabe 43.(2).

Ad (1). Es ist

$$f \;=\; [\bar{B} : \bar{A}] \;=\; [\bar{B} : \bar{B}_{\mathrm{inert}}] \cdot [\bar{B}_{\mathrm{inert}} : \bar{B}_{\mathrm{dec}}] \cdot [\bar{B}_{\mathrm{dec}} : \bar{A}] \overset{(2),\,\mathrm{L.}\,140.(2)}{=} [\bar{B}_{\mathrm{inert}} : \bar{B}_{\mathrm{dec}}] \,.$$

Da auch $[L_{\mathrm{inert}} : L_{\mathrm{dec}}] \overset{\mathrm{L.}\,141.(3)}{=} f$ ist, folgt $B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}_{\mathrm{inert}}$; cf. Aufgabe 43.(2). ▫

Wir fassen das Zerlegungsverhalten von $\mathfrak{p}$ bezüglich $\mathfrak{q}$ nochmals zusammen zum

Satz 143 (Hilbertscher Zerlegungssatz)

(1) *Es ist* $[L_{\mathrm{dec}} : K] = d$.
Es ist $\bar{A} = \bar{B}_{\mathrm{dec}}$ *(nach Identifikation). Es ist* $\mathrm{v}_{\mathfrak{q}_{\mathrm{dec}}}(B_{\mathrm{dec}}\mathfrak{p}) = 1$.

(2) *Es ist* $[L_{\mathrm{inert}} : L_{\mathrm{dec}}] = f$. *Es ist* $\mathrm{Gal}(L_{\mathrm{inert}}|L_{\mathrm{dec}}) \simeq G_{\mathfrak{q}}/I_{\mathfrak{q}} \simeq \mathrm{Gal}(\bar{B}|\bar{A})$.
Es ist $[\bar{B}_{\mathrm{inert}} : \bar{B}_{\mathrm{dec}}] = f$. *Es ist* $B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}} = \mathfrak{q}_{\mathrm{inert}}$.

(3) *Es ist* $[L : L_{\mathrm{inert}}] = e$. *Es ist* $\mathrm{Gal}(L|L_{\mathrm{inert}}) = I_{\mathfrak{q}}$.
Es ist $\bar{B}_{\mathrm{inert}} = \bar{B}$ *(nach Identifikation). Es ist* $B\mathfrak{q}_{\mathrm{inert}} = \mathfrak{q}^e$.

Beweis.

Ad (1). Dies folgt aus Lemmata 138.(4) und 140.(2, 1).

Ad (2). Dies folgt aus Lemmata 141.(3, 2) und 142.(1).

Ad (3). Dies folgt aus Lemmata 141.(3) und 142.(2). ▫

Wenn wir jeweils Trägheitsgrad und Verzweigungsindex in ein Paar schreiben und rechts die Galoisgruppen und die Grade notieren, können wir folgende grobe Übersicht geben.

$$\begin{array}{c} L \\ \big| \; e,\ \mathrm{Gal} = I_{\mathfrak{q}} \\ L_{\mathrm{inert}} \\ \big| \; f,\ \mathrm{Gal} \simeq G_{\mathfrak{q}}/I_{\mathfrak{q}} \\ L_{\mathrm{dec}} \\ \big| \; d \\ K \end{array} \qquad \begin{array}{l} \\ (1,e) \\ \\ (f,1) \\ \\ (1,1) \\ \end{array}$$

Beachte, daß im unteren Schritt hier nur Verzweigungsindex und Trägheitsgrad von $\mathfrak{q}_{\mathrm{dec}}$ gemeint sind, die da gleich 1 sein sollten, bei den anderen Primidealen, die in der Primidealfaktorzerlegung von $B_{\mathrm{dec}}\mathfrak{p}$ auftreten, haben wir hierüber ebensowenig Kontrolle wie insgesamt über die Zerlegungsbreite; cf. Aufgabe 62.

Beispiel 144 Wir greifen Beispiel 133 wieder auf und betrachten $\mathbf{Q}(\zeta_{120})|\mathbf{Q}$. Schreibe $\zeta := \zeta_{120}$. Für $k \in [0, 119]$ mit k teilerfremd zu 120 haben wir das Element $\sigma_k \in G := \mathrm{Gal}(\mathbf{Q}(\zeta)|\mathbf{Q})$ mit $\sigma_k(\zeta) = \zeta^k$.

Wir verwenden Querstriche, um Restklassenbildung modulo 3 zu notieren, für Polynome auch koeffizientenweise.

In $\mathbf{Z}[\zeta]$ ergab sich die Primidealfaktorzerlegung

$$(3) \;=\; (\zeta^4+\zeta^2+\zeta+1,\,3)^2(\zeta^4+\zeta^2+2\zeta+1,\,3)^2(\zeta^4+\zeta^3+\zeta^2+1,\,3)^2(\zeta^4+2\zeta^3+\zeta^2+1,\,3)^2\;.$$

Es ergab sich also $d=4$, $e=2$, $f=4$.

Sei $\mathfrak{q} := (\zeta^4+\zeta^2+\zeta+1,\,3)$ betrachtet.

Schreiben wir $g(X) := X^4+X^2+X+1 \in \mathbf{Z}[X]$, so wird $\mathfrak{q} = (g(\zeta),3)$. Da $\bar{g}(X)$ nach Konstruktion in Beispiel 133 ein Teiler von $\bar{\Phi}_{120}(X)$ ist, ist

$$\begin{array}{rcl} \mathbf{Z}[\zeta]/\mathfrak{q} & \xrightarrow{\sim} & \mathbf{F}_3[X]/(\bar{g}(X)) \\ \zeta+\mathfrak{q} & \longmapsto & X+(\bar{g}(X))\;; \end{array}$$

cf. Lösung zu Aufgabe 30.(2).

A priori ist $|G_\mathfrak{q}| = [L : L_{\mathrm{dec}}] = ef = 8$; cf. Lemma 138.(4) oder Satz 143.(2,3). Es ist

$$\begin{array}{rcl} G_\mathfrak{q} & = & \{\,\sigma\in G\,:\,\sigma(\mathfrak{q})=\mathfrak{q}\,\} \\ & = & \{\,\sigma\in G\,:\,\sigma(\mathfrak{q})\subseteq\mathfrak{q}\,\} \\ & = & \{\,\sigma\in G\,:\,\sigma(g(\zeta))\in\mathfrak{q}\,\} \\ & = & \{\,\sigma\in G\,:\,\sigma(g(\zeta))+\mathfrak{q}=0\,\}\;. \end{array}$$

Für $k\in[0,119]$ mit k teilerfremd zu 120 ist nun $\sigma_k(g(\zeta))+\mathfrak{q} = g(\zeta^k)+\mathfrak{q}$, was genau dann verschwindet, wenn das Bild $\bar{g}(X^k)+(\bar{g}(X))$ unter obigem Isomorphismus verschwindet, i.e. wenn $\bar{g}(X^k)$ in $\mathbf{F}_3[X]$ durch $\bar{g}(X)$ teilbar ist. Das können wir für jedes solche k ausrechnen und erhalten

$$G_\mathfrak{q} \;=\; \{\,\sigma_1\,,\,\sigma_{41}\,,\,\sigma_{43}\,,\,\sigma_{49}\,,\,\sigma_{67}\,,\,\sigma_{83}\,,\,\sigma_{89}\,,\,\sigma_{107}\,\}\;.$$

A priori ist $L_{\mathrm{dec}} = \mathrm{Fix}_{G_\mathfrak{q}}(\mathbf{Q}(\zeta))$ über $\mathbf{Q}$ von Grad $d=4$; cf. Satz 143.(1). Sicher liegt $\sum_{\sigma\in G_\mathfrak{q}}\sigma(\zeta) = -\zeta^{27}+\zeta^{21}-\zeta^9-\zeta^3 =: \xi$ in L_{dec}. Es ist $\mu_{\xi,\mathbf{Q}}(X) = X^4-4X^2+9$. Also ist bereits

$$\mathbf{Q}(\xi) \;=\; L_{\mathrm{dec}}\;.$$

> Die Bestimmung von $\mathcal{O}_{\mathbf{Q}(\xi)}$ kann etwa mit [4, §4.5.4] vorgenommen werden; wir lassen sie weg. Es würde sich $\mathbf{Z}[\xi]\subset\mathcal{O}_{\mathbf{Q}(\xi)}$ ergeben. Cf. auch Aufgabe 63.

A priori ist $|I_\mathfrak{q}| = [L : L_{\mathrm{inert}}] = e = 2$; cf. Satz 143.(3). Es ist

$$\begin{array}{rcl} I_\mathfrak{q} & = & \{\,\sigma\in G_\mathfrak{q}\,:\,\sigma(x)\equiv_\mathfrak{q} x \text{ für } x\in\mathbf{Z}[\zeta]\,\} \\ & = & \{\,\sigma\in G_\mathfrak{q}\,:\,\sigma(\zeta)\equiv_\mathfrak{q}\zeta\,\} \\ & = & \{\,\sigma\in G_\mathfrak{q}\,:\,\sigma(\zeta)-\zeta+\mathfrak{q}=0\,\}\;. \end{array}$$

Mit obigem Isomorphismus folgt, daß für $k\in\{1,41,43,49,67,83,89,107\}$ zunächst $\sigma_k(\zeta)=\zeta^k$ ist und sodann genau dann $\zeta^k-\zeta+\mathfrak{q}=0$ ist, wenn $X^k-X+(\bar{g}(X))=0$

ist, i.e. wenn $X^k - X$ in $\mathbf{F}_3[X]$ durch $\bar{g}(X)$ teilbar ist. Das können wir für jedes solche k ausrechnen und erhalten

$$I_{\mathfrak{q}} \;=\; \{\, \sigma_1 \,,\, \sigma_{41} \,\} \,.$$

A priori ist $L_{\text{inert}} = \text{Fix}_{I_{\mathfrak{q}}}(\mathbf{Q}(\zeta))$ über $\mathbf{Q}$ von Grad $df \;=\; 16$; cf. Satz 143.(1,2). Wegen $(\zeta^3)^{41} = \zeta^3$ liegt $\zeta^3 \in L_{\text{inert}}$. Da $\zeta^3 = \zeta_{120}^3 = \zeta_{40}$ ist und da $\varphi(40) = \varphi(8) \cdot \varphi(5) = 16$ ist, ist bereits

$$\mathbf{Q}(\zeta^3) \;=\; L_{\text{inert}} \,.$$

Anhang A

Aufgaben und Lösungen

A.1 Aufgaben

Aufgabe 1 (§1.1) Sei R ein kommutativer Ring.

(1) Finde einen surjektiven Ringmorphismus $S \longrightarrow\!\!\!\!\!\rightarrow R$ mit S Integritätsbereich.

(2) Wir setzen die Cramersche Regel über Körpern als bekannt voraus.
Leite daraus die Cramersche Regel über R ab.

Hinweis: Ringmorphismen wie in (1) sind mit der Cramerschen Regel verträglich. Jeder Integritätsbereich ist Teilring eines Körpers.

Aufgabe 2 (§1.1, Aufgabe 3) Sei R ein Hauptidealbereich. Sei $K := \mathrm{Quot}(R)$. Zeige.

(1) Sei M eine nichtleere Menge von Idealen von R. Es gibt in M ein maximales Element.

(2) Ein Element in $R^\times$ ist genau dann irreduzibel, wenn es prim ist.

(3) Sei $x \in R^\times$ gegeben.
Es gibt ein $n \geqslant 0$ und eine Faktorisierung $(x) = (p_1)(p_2)\cdots(p_n)$ mit p_i prim für alle $i \in [1, n]$; kurz, x hat eine Primfaktorzerlegung.
Sind $(x) = (p_1)(p_2)\cdots(p_n) = (p'_1)(p'_2)\cdots(p'_{n'})$ zwei Primfaktorzerlegungen, dann ist $n = n'$, und es gibt ein $\sigma \in \mathrm{S}_n$ mit $(p'_i) = (p_{\sigma(i)})$ für $i \in [1, n]$.

(4) Sei P die Menge der Primideale von R ungleich (0).
Sei $q \in R^\times$ prim. Definiere die *Bewertung* (engl. Valuation) bei q durch $\mathrm{v}_q : K^\times \longrightarrow\!\!\!\!\!\rightarrow \mathbf{Z}$ derart, daß für $x \in K^\times$ sich $x = e \prod_{(p)\in P} p^{\mathrm{v}_p(x)}$ ergibt, wobei $e \in \mathrm{U}(R)$ und wobei $\{\, (p) \in P \,:\, \mathrm{v}_p(x) \neq 0 \,\}$ endlich ist.
Wir setzen noch $\mathrm{v}_p(0) := \infty$, mit den Regeln $k \leqslant \infty$ und $k + \infty = \infty$ für $k \in \mathbf{Z} \sqcup \{\infty\}$.

(5) Seien x, $y \in K$. Es ist

$$\begin{aligned} \mathrm{v}_p(xy) &= \mathrm{v}_p(x) + \mathrm{v}_p(y) \\ \mathrm{v}_p(x+y) &\geqslant \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} \end{aligned}$$

In letzterem gilt Gleichheit, falls $\mathrm{v}_p(x) \neq \mathrm{v}_p(y)$.

(6) Sei $p \in R^\times$ prim. Ein Element $z \in K$ heiße *p-ganz*, falls $\mathrm{v}_p(z) \geqslant 0$.

(i) Die p-ganzen Elemente von K bilden einen Teilring.

(ii) Es ist genau dann $z \in R$, wenn z ein q-ganzes Element ist für alle $q \in R^\times$ prim.

(7) Gegeben $f(X) \in R[X]$ normiert. Ist $f(X) = g(X)h(X)$ mit $g(X)$, $h(X) \in K[X]$ normiert, dann sind $g(X)$, $h(X) \in R[X]$.

(8) Sei A ein Hauptidealbereich. Sei $K := \mathrm{Quot}(A)$. Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$. Sei $y \in L$ gegeben.

Es ist $y \in B$ genau dann, wenn $\mu_{y,K}(X) \in A[X]$ liegt.

Aufgabe 3 (§1.1)

Sei $d \in \mathbf{Z} \smallsetminus \{0, 1\}$ quadratfrei, d.h. sei $\mathrm{v}_p(d) \in \{0, 1\}$ für alle $p \in \mathbf{Z}^\times$ prim.

Sei $K := \mathbf{Q}(\sqrt{d})$.

Bestimme $\mathcal{O}_K$.

Was ergibt sich speziell im Falle $K = \mathbf{Q}(\mathrm{i})$? Im Falle $K = \mathbf{Q}(\sqrt{5})$? Im Falle $K = \mathbf{Q}(\zeta_3)$?

Aufgabe 4 (§1.1) Sei $p \in \mathbf{Z}_{\geqslant 3}$ eine Primzahl.

Schreibe $\mathcal{Z} = \mathbf{F}_p[T]$ und $\mathcal{Q} = \mathbf{F}_p(T)$. Sei $d(T) \in \mathcal{Z}$ quadratfrei.

Gib eine $\mathcal{Z}$-lineare Basis von $\Gamma_{\mathcal{Q}\left(\sqrt{d(T)}\right)}(\mathcal{Z})$ an.

Aufgabe 5 (§1.1) Seien $T|S|R$ Erweiterungen kommutativer Ringe. Zeige.

(1) Ist $T|S$ ganz und $S|R$ ganz, dann ist auch $T|R$ ganz.

(2) Sei $A \subseteq R$ ein Teilring. Sei $B := \Gamma_S(A)$. Es ist $\Gamma_T(A) = \Gamma_T(B)$.

Aufgabe 6 (§1.1)

(1) Sei R ein Hauptidealbereich. Zeige, daß R ganzabgeschlossen ist.

(2) Zeige, daß $\mathbf{Z}[\mathrm{i}]$ ein Hauptidealbereich ist.

(3) Zeige, daß $\mathbf{Z}[\zeta_3]$ ein Hauptidealbereich ist.

(4) Zeige, daß $\mathbf{Z}[\sqrt{-5}]$ kein Hauptidealbereich ist. Ist $\mathbf{Z}[\sqrt{-5}]$ ganzabgeschlossen?

Aufgabe 7 (§1.2) Zeige.

(1) Es ist $\mathbf{Q}(\sqrt[3]{2},\zeta_3)|\mathbf{Q}$ galoisch mit $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\zeta_3)|\mathbf{Q})$ isomorph zur symmetrischen Gruppe S_3. Bestimme alle Zwischenkörper dieser Erweiterung.

(2) Es ist $\mathbf{Q}(\sqrt[3]{2},\zeta_3)$ Zerfällungskörper von $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$.

(3) Es ist $\mathbf{Q}(\sqrt[3]{2},\zeta_3)$ nicht Zerfällungskörper von $\mathbf{Q}(\zeta_3)|\mathbf{Q}$.

(4) Berechne $\mathrm{Tr}_{\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}}(\sqrt[3]{2})$ und $\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}}(\sqrt[3]{2})$ jeweils einmal nach Definition und einmal unter Verwendung von Lemma 15.

Aufgabe 8 (§1.2) Sei K perfekt. Sei $L|K$ eine endliche Erweiterung.

Zeige, daß L perfekt ist.

Aufgabe 9 (§1.2) Wir betrachten $U := \mathrm{S}_3 \leqslant \mathrm{S}_4 =: G$.

(1) Wieviele Teilmengen $T \subseteq \mathrm{S}_4$ gibt es mit $G = \bigsqcup_{\sigma\in T} \sigma U$?

(2) Finde unter den Teilmengen von (1) zwei, die zueinander nichtisomorphe Untergruppen von G sind.

Aufgabe 10 (§2.3) Sei A ein Integritätsbereich. Sei $K := \mathrm{Quot}(A)$. Zeige.

(1) Sei $S \subseteq A^\times$ mit $1 \in S$ und mit $st \in S$ für $s,\, t \in S$ gegeben. Sei $\mathfrak{a} \subseteq A$ ein Ideal. Sei

$$S^{-1}\mathfrak{a} \;:=\; \{\, \frac{a}{s} \in K \,:\, a \in \mathfrak{a},\, s \in S \,\} \;\subseteq\; K$$

Es sind $A \subseteq S^{-1}A \subseteq K$ Inklusionen von Teilringen.

Für jeden kommutativen Ring B und jeden Ringmorphismus $\varphi : A \longrightarrow B$ mit $\varphi(S) \subseteq \mathrm{U}(B)$ gibt es genau einen Ringmorphismus $\psi : S^{-1}A \longrightarrow B$ mit $\psi|_A = \varphi$.

Es ist $S^{-1}\mathfrak{a} \subseteq S^{-1}A$ ein Ideal.

Sei $\mathrm{Ideale}^{A\smallsetminus S}_{\mathrm{prim}}(A)$ die Menge der Primideale von A, die leeren Schnitt mit S haben.

Es gibt eine Bijektion von $\mathrm{Ideale}^{A\smallsetminus S}_{\mathrm{prim}}(A)$ nach $\mathrm{Ideale}_{\mathrm{prim}}(S^{-1}A)$.

(2) Sei $\mathfrak{p} \subseteq A$ ein Primideal. Sei $S := A \smallsetminus \mathfrak{p}$. Für ein Ideal $\mathfrak{a} \subseteq A$ setzen wir $\mathfrak{a}_\mathfrak{p} := S^{-1}\mathfrak{a}$.

Die Primideale von A, die in $\mathfrak{p}$ liegen, stehen in Bijektion zu den Primidealen von $A_\mathfrak{p}$.

Es ist $\mathfrak{p}_\mathfrak{p}$ das einzige maximale Ideal in $A_\mathfrak{p}$.

Es ist $\mathrm{Quot}(A/\mathfrak{p})$ isomorph zu $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$.

Ist $\mathfrak{p} \subseteq A$ maximal, dann ist $A/\mathfrak{p}$ isomorph zu $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$.

Aufgabe 11 (§1.1) Zeige.

(1) Sei L ein Körper. Sei $A \xrightarrow{\varphi} L$ die Einbettung eines Teilrings. Es gibt genau einen Körpermorphismus $\mathrm{Quot}(A) \xrightarrow{\psi} L$ mit $\psi|_A = \varphi$.

(2) Sei A ein Integritätsbereich. Sei $A \subseteq B \subseteq \mathrm{Quot}(A)$, mit B Teilring von $\mathrm{Quot}(A)$. Wir haben den Isomorphismus $\mathrm{Quot}(A) \longrightarrow \mathrm{Quot}(B)$, $x/y \longmapsto x/y$, wobei $x \in A$ und $y \in A^\times$.

Aufgabe 12 (§1.3.3) Zeige oder widerlege.

Sei K ein perfekter Körper. Sei $L|K$ eine endliche Körpererweiterung.

Sei $A \subseteq K$ ein ganzabgeschlossener Teilring mit $K = \mathrm{Quot}(A)$. Sei $B := \Gamma_L(A)$.

Für $y \in L$ liegt genau dann $y \in \mathrm{U}(B)$, wenn $\mathrm{N}_{L|K}(y) \in \mathrm{U}(A)$ liegt.

Aufgabe 13 (§1.3.3)

(1) Sei R ein kommutativer Ring mit $1_R \neq 0_R$. Seien k, $\ell \geqslant 0$ mit $R^{\oplus k} \simeq R^{\oplus \ell}$ gegeben. Zeige $k = \ell$.

Ist M ein R-Modul mit $M \simeq R^{\oplus k}$ für ein $k \geqslant 0$, so heißt M *endlich erzeugt frei* und $\mathrm{rk}_R(M) := k$ der *Rang* von M.

(2) Sei R ein Hauptidealbereich. Sei M ein endlich erzeugt freier R-Modul. Sei $N \subseteq M$ ein Teilmodul. Zeige, daß auch N ein endlich erzeugt freier R-Modul ist mit $\mathrm{rk}_R(N) \leqslant \mathrm{rk}_R(M)$.

Aufgabe 14 (§1.3.2) Zeige.

(1) Sei $n \geqslant 0$. Sei $A \in \mathbf{Z}^{n\times n}$ mit $\det(A) \neq 0$. Dann ist $|\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1}| = |\det(A)|$.

(2) Sei $n \geqslant 0$. Sei X ein endlich erzeugt freier $\mathbf{Z}$-Modul mit $\mathbf{Z}$-linearer Basis $\underline{x} = (x_i : i \in [1,n])$. Sei $Y \subseteq X$ ein $\mathbf{Z}$-Teilmodul mit $\mathbf{Z}$-linearer Basis $\underline{y} = (y_j : j \in [1,n])$. Sei $y_j = \sum_{i\in[1,n]} a_{i,j}x_i$ für $j \in [1,n]$, wobei $A := (a_{i,j})_{i,j} \in \mathbf{Z}^{n\times n}$.
Dann ist $|X/Y| = |\det(A)|$.

(3) Sei $K|\mathbf{Q}$ eine endliche Körpererweiterung. Sei $\underline{y} := (\, y_i \,:\, i \in [1,n]\,)$ eine $\mathbf{Q}$-lineare Basis von K, die in $\mathcal{O}_K$ liegt. Sei $Y := {}_{\mathbf{Z}}\langle \underline{y} \rangle \subseteq K$. Dann ist $Y \subseteq Y^\#$ und es wird $|Y^\#/Y| = |\Delta_{K|\mathbf{Q},\underline{y}}|$.

Aufgabe 15 (§1.3.3) Zeige oder widerlege.

Sei $L|K$ eine endliche Körpererweiterung mit K perfekt. Schreibe $\ell := [L : K]$. Sei $A \subseteq K$ ein ganzabgeschlossener Teilring mit $\mathrm{Quot}(A) = K$. Sei $B \subseteq \Gamma_L(A)$ ein Teilring.

Sei $\underline{g} := (\, g_i \,:\, i \in [1,\ell]\,)$ eine K-lineare Basis von L mit $B = {}_A\langle \underline{g} \rangle$.

(1) Ist $[L:K]$ ungerade, dann ist $\det(\mathrm{Vand}_{L|K,\underline{g}}) \in A$.

(2) Ist $L|K$ galoisch und $[L:K]$ ungerade, dann ist $\det(\mathrm{Vand}_{L|K,\underline{g}}) \in A$.

Aufgabe 16 (§1.3.3, §1.4.3) Berechne folgende Diskriminanten.

(1) $\Delta_{\mathbf{Q}(\sqrt{d})}$ für $d \in \mathbf{Z} \smallsetminus \{0,1\}$ quadratfrei.

(2) $\Delta_{\mathbf{Q}(\sqrt{3},\sqrt{13})}$.

Aufgabe 17 (§4.1)

(1) Sei $n \geqslant 1$. Zeige, daß $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ galoisch ist, mit einem Gruppenisomorphismus

$$\begin{array}{rcl} \mathrm{U}(\mathbf{Z}/(n)) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbf{Q}(\zeta_n)|\mathbf{Q}) \\ k+(n) & \longmapsto & (\zeta_n \mapsto \zeta_n^k)\,. \end{array}$$

(2) Für $n \geqslant 1$ sei $\Phi_n(X) := \mu_{\zeta_n,\mathbf{Q}}(X) \in \mathbf{Z}[X]$ das n-te Kreisteilungspolynom. Zeige

$$X^n - 1 \;=\; \prod_{d \in \mathbf{Z}_{\geqslant 1},\, n \equiv_d 0} \Phi_d(X)\,.$$

Aufgabe 18 (§1.3.3, Aufgabe 14) Sei $K|\mathbf{Q}$ eine endliche Körpererweiterung.

Ein $\mathbf{Z}$-*Gitter* in K ist ein $\mathbf{Z}$-Teilmodul von K von der Form ${}_{\mathbf{Z}}\langle\underline{y}\rangle$ für eine $\mathbf{Q}$-lineare Basis $\underline{y}$ von K.

Eine $\mathbf{Z}$-*Ordnung* in K ist ein $\mathbf{Z}$-Gitter in K, das zudem ein Teilring ist.

(1) Zeige. Es ist $\mathcal{O}_K$ eine $\mathbf{Z}$-Ordnung in K. Jede $\mathbf{Z}$-Ordnung in K liegt in $\mathcal{O}_K$.

(2) Seien G und H zwei $\mathbf{Z}$-Gitter in K mit $G \subseteq H$.
Zeige, daß $|H/G|$ endlich und gleich $|G^\#/H^\#|$ ist.

(3) Sei R eine $\mathbf{Z}$-Ordnung in K. Schreibe $R = {}_{\mathbf{Z}}\langle\underline{y}\rangle$ für eine $\mathbf{Q}$-lineare Basis $\underline{y}$ von K. Sei $\Delta_{K|\mathbf{Q},\underline{y}}$ quadratfrei.
Zeige $R = \mathcal{O}_K$.

(4) Sei $\alpha \in \mathbf{C}$ eine Nullstelle des irreduziblen Polynoms $X^3 + X + 1 \in \mathbf{Q}[X]$. Sei $K := \mathbf{Q}(\alpha)$. Zeige $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Berechne Δ_K.

Aufgabe 19 (§1.3.3) Betrachte $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$. Schreibe $\delta := \sqrt[3]{2}$.

(1) Bestimme $\mathbf{Z}[\delta]^\#$.

(2) Zeige $\mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$. Bestimme $\Delta_{\mathbf{Q}(\delta)}$.

Aufgabe 20 (§1.4.2) Sei K ein perfekter Körper.

Seien $L'|K$ und $L''|K$ linear disjunkte endliche Körpererweiterungen.

Sei $L|K$ ein Kompositum von $L'|K$ und $L''|K$, mittels $\varphi' : L' \longrightarrow L$ und $\varphi'' : L'' \longrightarrow L$. Zeige.

(1) Ist $\tilde{L}|K$, mit $\tilde{\varphi}'$, $\tilde{\varphi}''$, ein weiteres Kompositum von $L'|K$ und $L''|K$, dann gibt es einen eindeutigen Körpermorphismus $\alpha : L \xrightarrow{\sim} \tilde{L}$ mit $\alpha \circ \varphi' = \tilde{\varphi}'$ und $\alpha \circ \varphi'' = \tilde{\varphi}''$, und dieser ist ein Isomorphismus.

(2) Ist $M|K$ eine endliche Körpererweiterung und sind Körpermorphismen $L' \xrightarrow{\psi'} M$ und $L'' \xrightarrow{\psi''} M$ mit $\psi'|_K^K = \psi''|_K^K = \mathrm{id}_K$ gegeben, dann gibt es einen eindeutigen Körpermorphismus $\beta : L \longrightarrow M$ mit $\beta \circ \varphi' = \psi'$ und $\beta \circ \varphi'' = \psi''$.

Aufgabe 21 (§1.4.3) Sei K ein Körper. Seien m, $n \geqslant 0$. Sei $A := (a_{i,j})_{i,j} \in K^{m \times m}$.

Sei $\alpha : [1, mn] \xrightarrow{\sim} [1, m] \times [1, n]$, $k \longmapsto \alpha(k) =: (\alpha'(k), \alpha''(k))$ eine Bijektion.

Sei $B := (a_{\alpha'(k),\alpha'(\ell)} \partial_{\alpha''(k),\alpha''(\ell)})_{k,\ell} \in K^{mn \times mn}$.

Zeige $\det(B) = \det(A)^n$.

Aufgabe 22 (§1.3.3) Sei $K|\mathbf{Q}$ eine endliche Körpererweiterung.

Zeige, daß $\Delta_K \equiv_4 0$ oder $\Delta_K \equiv_4 1$ ist.

Hinweis: Schreibe $\det(\mathrm{Vand}_{K|\mathbf{Q},\underline{g}}) = P - N$, wobei in P die Terme aus der Leibnizformel mit positivem Vorzeichen stehen. Zeige, daß $P + N$ und PN in $\mathbf{Z}$ liegen.

Aufgabe 23 (§1.2.1, §1.4.1, §1.4.2) Zeige oder widerlege.

Sei K ein perfekter Körper.

Sei $L|K$ eine endliche Körpererweiterung.

Seien $L|L'|K$ und $L|L''|K$. Sei $L|K$ Kompositum von $L'|K$ und $L''|K$, via der Einbettungen.

Sei E ein Zerfällungskörper von $L|K$. Sei E' ein Zerfällungskörper von $L'|K$. Sei E'' ein Zerfällungskörper von $L''|K$.

(1) Sind $L'|K$ und $L''|K$ linear disjunkt, dann sind auch $E'|K$ und $E''|K$ linear disjunkt.

(2) Es ist $E|K$ ein Kompositum von E' und E'', via geeigneter Körpermorphismen.

(3) Sind $L'|K$ und $L''|K$ galoisch, dann auch $L|K$.

(4) Sind $[L' : K]$ und $[L'' : K]$ teilerfremd, dann sind $L'|K$ und $L''|K$ linear disjunkt.

(5) Seien $L'|K$ und $L''|K$ galoisch. Es sind $L'|K$ und $L''|K$ linear disjunkt genau dann, wenn $L' \cap L'' = K$ ist.

(6) Es sind $L'|K$ und $L''|K$ linear disjunkt genau dann, wenn $L' \cap L'' = K$ ist.

Aufgabe 24 (§2.1) Sei R ein kommutativer Ring. Zeige.

(1) Die folgenden Aussagen (i) und (ii) sind äquivalent.
   (i) Jedes Ideal in R ist endlich erzeugt.
   (ii) Jede nichtleere Teilmenge von $\mathrm{Ideale}(R)$ hat ein maximales Element.

(2) Ist R noethersch, dann ist auch $R[X]$ noethersch.

(3) Ist R noethersch und $\mathfrak{a} \in \mathrm{Ideale}(R)$, dann ist auch $R/\mathfrak{a}$ noethersch.

(4) Sei R noethersch. Sei $m \geqslant 0$.
Sei $N \subseteq R^{\oplus m}$ ein R-Teilmodul. Dann ist N ein endlich erzeugter R-Modul.

(5) Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt. Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$.
Dann ist B noethersch. Ferner ist B ein endlich erzeugter A-Modul.

(6) Es ist $\prod_{k \in \mathbf{Z}_{\geqslant 1}} \mathbf{C}$, mit eintragsweiser Addition und Multiplikation, nicht noethersch.

(7) Es ist $\mathbf{C}[X, Y]$ noethersch. Der Teilring darin, der von den Elementen XY^k mit $k \geqslant 0$ erzeugt wird, ist nicht noethersch, da in diesem Teilring das Ideal, das von ebendiesen Elementen erzeugt wird, nicht endlich erzeugt ist.

Aufgabe 25 (§2.2) Sei A ein ganzabgeschlossener Integritätsbereich. Sei $K := \mathrm{Quot}(A)$. Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$. Zeige.

(1) Sei $f(X) \in A[X]$ normiert. Ist $f(X) = g(X)h(X)$ mit $g(X), h(X) \in K[X]$, dann liegen $g(X), h(X) \in A[X]$.

(2) Sei $y \in L$. Es ist $y \in B$ genau dann, wenn $\mu_{y,K}(X) \in A[X]$ liegt.

Aufgabe 26 (§2.3.1) Zeige.

(1) Sei R ein kommutativer Ring. Sei $n \geqslant 1$. Sei $\mathfrak{a}_i \in \mathrm{Ideale}(R)$ für $i \in [1, n]$. Sei $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i, j \in [1, n]$ mit $i \neq j$. Der Ringmorphismus

$$\begin{array}{ccc} R & \xrightarrow{\chi} & \prod_{i \in [1,n]} R/\mathfrak{a}_i \\ r & \longmapsto & (r + \mathfrak{a}_i)_i \end{array}$$

ist surjektiv. Hierbei seien Addition und Multiplikation auf $\prod_{i \in [1,n]} R/\mathfrak{a}_i$ eintragsweise erklärt.

(2) Sei D ein Dedekindbereich. Sei $n \geqslant 1$. Seien $\mathfrak{p}_i \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$ mit $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i, j \in [1,n]$ mit $i \neq j$, und seien $k_i \geqslant 1$ für $i \in [1,n]$. Der Ringmorphismus

$$\begin{array}{ccc} D & \xrightarrow{\chi} & \prod_{i\in[1,n]} D/\mathfrak{p}_i^{k_i} \\ d & \longmapsto & (d+\mathfrak{p}_i)_i \end{array}$$

ist surjektiv.

Aufgabe 27 (§2.2)

(1) Finde $\mathfrak{a} \in \mathrm{Ideale}^\times(\mathbf{Z}[\sqrt{-5}])$ mit $\mathfrak{a}$ kein Hauptideal, aber $\mathfrak{a}^2$ Hauptideal.

(2) Faktorisiere in $\mathbf{Z}[\sqrt{-5}]$ das Ideal (21) in Primideale. Faktorisiere es auf drei wesentlich verschiedene Weisen in ein Produkt von Hauptidealen, die von irreduziblen Elementen erzeugt werden. Zerlege die letzteren Faktorisierungen weiter zur Primidealfaktorzerlegung.

(3) Finde einen Zahlkörper K und eine Primzahl $p \in \mathbf{Z}^\times$ so, daß in der Primidealfaktorzerlegung von $(p) \subseteq \mathcal{O}_K$ ein Faktor $\mathfrak{p}$ mit Exponent $\geqslant 2$ auftritt.
   (i) Hierbei soll $\mathfrak{p}$ kein Hauptideal sein.
   (ii) Hierbei soll $\mathfrak{p}$ ein Hauptideal sein.

Aufgabe 28 (§2.2)

(1) Sei D ein Dedekindbereich. Seien $\mathfrak{g}, \mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(D)$.
   Dann sind auch $\mathfrak{gh}$, $\mathfrak{g}\cap\mathfrak{h}$, $\mathfrak{g}+\mathfrak{h}$, $\mathfrak{g}^{-1} \in \underline{\mathrm{Ideale}}^\times(D)$.
   Ist $\mathfrak{g} \subseteq D$, dann ist $\mathfrak{g} \in \mathrm{Ideale}^\times(D)$.
   Sind bereits $\mathfrak{g}, \mathfrak{h} \in \mathrm{Ideale}^\times(D)$, dann sind auch $\mathfrak{gh}$, $\mathfrak{g}\cap\mathfrak{h}$, $\mathfrak{g}+\mathfrak{h} \in \mathrm{Ideale}^\times(D)$.

(2) Sei R ein kommutativer Ring. Sei $\mathfrak{p} \in \mathrm{Ideale}_{\mathrm{prim}}(R)$. Seien $\mathfrak{a}, \mathfrak{b} \in \mathrm{Ideale}(R)$.
   Es ist $\mathfrak{ab} \subseteq \mathfrak{p}$ genau dann, wenn $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ ist.

Aufgabe 29 (§2.2) Sei D ein Dedekindbereich. Sei $K := \mathrm{Quot}(D)$.

Sei $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$. Seien $\mathfrak{g}, \mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(D)$. Seien $\mathfrak{a}, \mathfrak{b} \in \mathrm{Ideale}^\times(D)$. Sei $S \subseteq D^\times$ mit $1 \in S$ und mit $st \in S$ für $s, t \in S$.

(1) Sei $k \geqslant 0$. Zeige, daß genau dann $\mathfrak{a} \subseteq \mathfrak{p}^k$ ist, wenn $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geqslant k$ ist.

(2) Schreibe $\gamma := \mathrm{v}_\mathfrak{p}(\mathfrak{g})$ und $\chi := \mathrm{v}_\mathfrak{p}(\mathfrak{h})$. Wie hängen $\mathrm{v}_\mathfrak{p}(\mathfrak{gh})$, $\mathrm{v}_\mathfrak{p}(\mathfrak{g}^{-1})$, $\mathrm{v}_\mathfrak{p}(\mathfrak{g}\cap\mathfrak{h})$, $\mathrm{v}_\mathfrak{p}(\mathfrak{g}+\mathfrak{h})$ von γ und χ ab?

(3) Seien $x, y \in K^\times$. Zeige $\mathrm{v}_\mathfrak{p}(xy) = \mathrm{v}_\mathfrak{p}(x) + \mathrm{v}_\mathfrak{p}(y)$. Zeige $\mathrm{v}_\mathfrak{p}(x+y) \geqslant \min\{\mathrm{v}_\mathfrak{p}(x), \mathrm{v}_\mathfrak{p}(y)\}$, wobei Gleichheit gilt, falls $\mathrm{v}_\mathfrak{p}(x) \neq \mathrm{v}_\mathfrak{p}(y)$.

(4) Zeige, daß genau dann $\mathfrak{a} + \mathfrak{b} = (1)$ ist, wenn es kein $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ gibt, das in der Primidealfaktorzerlegung von $\mathfrak{a}$ und von $\mathfrak{b}$ als Faktor auftritt.

(5) Zeige, daß es $x,\, y \in D$ gibt mit $\mathfrak{a} = (x, y)$.

(6) Sei $\mathfrak{a} + \mathfrak{b} = (1)$. Zeige, daß $\mathfrak{ab} \oplus D$ und $\mathfrak{a} \oplus \mathfrak{b}$ als D-Moduln isomorph sind.

(7) Zeige, daß $\mathfrak{a} \oplus \mathfrak{a}^{-1}$ und $D \oplus D$ als D-Moduln isomorph sind. Ist $\mathfrak{a}$ in eine direkte Summe von echten D-Teilmoduln zerlegbar? Wann ist $\mathfrak{a}$ isomorph zu D als D-Modul?

(8) Zeige $S^{-1}(\mathfrak{ab}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$, $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (S^{-1}\mathfrak{a}) \cap (S^{-1}\mathfrak{b})$ und $S^{-1}(\mathfrak{a} + \mathfrak{b}) = (S^{-1}\mathfrak{a}) + (S^{-1}\mathfrak{b})$. Zeige $\mathfrak{a}_{\mathfrak{p}} = (\mathfrak{p}_{\mathfrak{p}})^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})}$.

Aufgabe 30 (§2.2) Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$.

Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$.

(1) Sei $C|A$ eine Erweiterung kommutativer Ringe. Sei $\mathfrak{a} \subseteq A$ eine Teilmenge. Sei $\mathfrak{c} \in \mathrm{Ideale}(C)$. Zeige $\mathfrak{a} \cdot \mathfrak{c} := {}_{\mathbf{Z}}\langle\, ac \,:\, a \in \mathfrak{a},\, c \in \mathfrak{c} \,\rangle \in \mathrm{Ideale}(C)$.

(2) Sei $\mathfrak{a} \in \mathrm{Ideale}(A)$. Schreibe $\bar{A} := A/\mathfrak{a}$ und $\bar{a} := a + \mathfrak{a} \in \bar{A}$ für $a \in A$. Sei $b \in B$. Sei $\mu_{b,K}(X) =: X^n + \sum_{i\in[0,n-1]} a_i X^i$. Schreibe $\bar{\mu}_{b,K}(X) := X^n + \sum_{i\in[0,n-1]} \bar{a}_i X^i$. Zeige.

(i) Wir haben einen Ringisomorphismus $\varphi : A[b]/(\mathfrak{a} \cdot A[b]) \xrightarrow{\sim} \bar{A}[X]/(\bar{\mu}_{b,K}(X))$ mit $\varphi(a + (\mathfrak{a} \cdot A[b])) = \bar{a} + (\bar{\mu}_{b,K}(X))$ für $a \in A$ und mit $\varphi(b + (\mathfrak{a} \cdot A[b])) = X + (\bar{\mu}_{b,K}(X))$.

(ii) Sei $\mathfrak{a}$ ein maximales Ideal von A. Beachte, daß nun $\bar{A}$ ein Körper ist.
Schreibe
$$\bar{\mu}_{b,K}(X) = \bar{u}_1(X)^{\alpha_1} \cdot \bar{u}_2(X)^{\alpha_2} \cdot \ldots \cdot \bar{u}_k(X)^{\alpha_k}$$
für ein $k \geqslant 1$, normierte Polynome $u_i(X) \in A[X]$ für $i \in [1,k]$, für welche $\bar{u}_i(X) \in \bar{A}[X]$ irreduzibel ist, wobei $\bar{u}_i(X) \neq \bar{u}_j(X)$ für $i,\, j \in [1,k]$ mit $i \neq j$, und für gewisse $\alpha_i \geqslant 1$ für $i \in [1,n]$.
Dann sind die maximalen Ideale über $\mathfrak{a}$ in $A[b]$ gegeben durch
$$\mathfrak{q}_i \;:=\; (u_i(b)) + \mathfrak{a}A[b]$$
für $i \in [1,k]$. Desweiteren ist $A[b]/\mathfrak{q}_i \xrightarrow{\sim} \bar{A}[X]/(\bar{u}_i(X))$, $b + \mathfrak{q}_i \longmapsto X + (\bar{u}_i(X))$ und also
$$[A[b]/\mathfrak{q}_i : \bar{A}] \;=\; [\bar{A}[X]/(\bar{u}_i(X)) : \bar{A}] \;=\; \deg(\bar{u}_i)$$
für $i \in [1,k]$.

(iii) Wir behalten die Bezeichnungen aus (ii) bei. Sei zudem vorausgesetzt, daß $A[b] = B$ ist. Dann ist
$$\mathfrak{a} \cdot A[b] \;=\; \mathfrak{q}_1^{\alpha_1}\mathfrak{q}_2^{\alpha_2} \cdot \ldots \cdot \mathfrak{q}_k^{\alpha_k}\ .$$

(3) Sei $d \in \mathbf{Z} \setminus \{0,1\}$ quadratfrei. Sei $p \in \mathbf{Z}^\times$ prim. Gib die Primidealfaktorzerlegung von $(p) \subseteq \mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ an. Hierbei darf $(\mathbf{F}_p^\times)^2 := \{ s^2 : s \in \mathbf{F}_p^\times \}$ als bekannt vorausgesetzt werden. Was ergibt sich speziell für $d = -1$ und $p \in \{2,3,5\}$?

(4) Finde jeweils die Primidealfaktorzerlegung von (2), (3), (5), (7) $\subseteq \mathcal{O}_{\mathbf{Q}(\sqrt[3]{2})}$.

Aufgabe 31 (§2.3.1) Sei A ein Dedekindbereich mit $K := \mathrm{Quot}(A)$ perfekt.
Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$. Gebe es ein $b \in B$ mit $B = A[b]$.
Sei $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$. Zeige $B_\mathfrak{p} = A_\mathfrak{p}[b]$.

Aufgabe 32 (§2.3.1, §2.1) Finde einen Hauptidealbereich A mit $|\,\mathrm{Ideale}^\times_{\mathrm{prim}}(A)| = 2$.

Aufgabe 33 (§2.3.2) Sei D ein Dedekindbereich. Sei $S \subseteq D$ mit $1 \in S$ und $st \in S$ für $s, t \in D$ gegeben; cf. Aufgabe 10. Seien $\mathfrak{g}, \mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(D)$ gegeben. Zeige.

(1) Es ist $S^{-1}\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(S^{-1}D)$.

(2) Es ist $S^{-1}(\mathfrak{g}\mathfrak{h}) = (S^{-1}\mathfrak{g})(S^{-1}\mathfrak{h})$ und $(S^{-1}\mathfrak{g})^{-1} = S^{-1}(\mathfrak{g}^{-1})$.

(3) Es ist $S^{-1}(\mathfrak{g}+\mathfrak{h}) = S^{-1}\mathfrak{g} + S^{-1}\mathfrak{h}$ und $S^{-1}(\mathfrak{g}\cap\mathfrak{h}) = S^{-1}\mathfrak{g} \cap S^{-1}\mathfrak{h}$.

(4) Sei $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$. Es ist $\mathfrak{g}_\mathfrak{p} = (\mathfrak{p}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}(\mathfrak{g})}$.

(5) Es ist $\mathfrak{g} = \bigcap_{\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(D)} \mathfrak{g}_\mathfrak{p}$.

Aufgabe 34 (§2.3.3) Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt.
Seien $M|L|K$ endliche Körpererweiterungen. Sei $B := \Gamma_L(A)$ und $C := \Gamma_M(A)$.
Zeige.

(1) Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$. Dann ist $\mathrm{N}_{L|K}(\mathfrak{g}^{-1}) = \mathrm{N}_{L|K}(\mathfrak{g})^{-1}$.

(2) Sei $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(C)$. Dann ist $\mathrm{N}_{M|K}(\mathfrak{h}) = \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\mathfrak{h}))$.

(3) Sei $\mathfrak{f} \in \underline{\mathrm{Ideale}}^\times(A)$. Dann ist $\mathrm{N}_{L|K}(\mathfrak{f}B) = \mathfrak{f}^\ell$, wobei $\ell := [L:K]$.

Aufgabe 35 (§2.3.4) Zeige oder widerlege.
Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt.
Seien $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$.

(1) Es ist $B^{\#,A}$ das Urbild von A unter $\mathrm{Tr}_{L|K}$.

(2) Für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ ist $(B^{\#,A})_\mathfrak{p} = (B_\mathfrak{p})^{\#,A_\mathfrak{p}}$.

(3) Für $x,\, y \in L^\times$ ist $\mathrm{N}_{L|K}(\,(x,y)\,) = (\,\mathrm{N}_{L|K}(x),\, \mathrm{N}_{L|K}(y)\,)$.

(4) Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ ist $\mathrm{N}_{L|K}(\mathfrak{b}) \subseteq \mathfrak{b} \cap A$.

(5) Sei $L|K$ galoisch. Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ ist $\mathrm{N}_{L|K}(\mathfrak{b}) = \mathfrak{b} \cap A$.

(6) Die Abbildung $\mathrm{N}_{L|K} : \underline{\mathrm{Ideale}}^\times(B) \longrightarrow \underline{\mathrm{Ideale}}^\times(A)$ ist injektiv.

(7) Die Abbildung $\mathrm{N}_{L|K} : \underline{\mathrm{Ideale}}^\times(B) \longrightarrow \underline{\mathrm{Ideale}}^\times(A)$ ist surjektiv.

(8) Sei $L|K$ galoisch, mit $G := \mathrm{Gal}(L|K)$.
Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ ist $\mathrm{N}_{L|K}(\mathfrak{b})B = \prod_{\sigma\in G} \sigma(\mathfrak{b})$.

(9) Für $\mathfrak{a} \in \mathrm{Ideale}^\times(A)$ ist $(B\mathfrak{a}) \cap A = \mathfrak{a}$.

(10) Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$. Es ist $\mathrm{N}_{L|K}(\mathfrak{g}) = \{\, \mathrm{N}_{L|K}(g) \,:\, g \in \mathfrak{g} \,\}$.

(11) Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(B)$. Es ist $\mathrm{N}_{L|K}(\mathfrak{g}) = (1)$ genau dann, wenn $\mathfrak{g} = (1)$ ist.

(12) Sei $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$. Es ist $\mathrm{N}_{L|K}(\mathfrak{b}) = (1)$ genau dann, wenn $\mathfrak{b} = (1)$ ist.

Aufgabe 36 (§2.3.3, §2.2, Aufgabe 47) Zeige.

(1) In $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})})$ hat das Element $[(2, \frac{1}{2}(1+\sqrt{-23}))]$ die Ordnung 3.

(2) In $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-47})})$ hat das Element $[(2, \frac{1}{2}(1+\sqrt{-47}))]$ die Ordnung 5.

Aufgabe 37 (§2.3.3) Zeige oder widerlege.
Sei A ein Dedekindbereich mit $K := \mathrm{Quot}(A)$ perfekt.
Sei $L|K$ eine endliche Körpererweiterung. Sei $B := \Gamma_L(A)$.
Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ betrachten wir $\mathrm{Tr}_{L|K}(\mathfrak{b}) = \{\, \mathrm{Tr}_{L|K}(b) \,:\, b \in \mathfrak{b} \,\}$.

(1) Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ ist $B(\mathfrak{b} \cap A) = \mathfrak{b}$.

(2) Für $\mathfrak{b},\, \mathfrak{b}' \in \mathrm{Ideale}^\times(B)$ ist $A \cap (\mathfrak{b}\mathfrak{b}') = (A \cap \mathfrak{b})(A \cap \mathfrak{b}')$.

(3) Für $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$ ist $\mathrm{Tr}_{L|K}(\mathfrak{b}) \in \mathrm{Ideale}^\times(A)$.

(4) Für $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(B)$ ist $\mathrm{Tr}_{L|K}(\mathfrak{h}) \in \underline{\mathrm{Ideale}}^\times(A)$.

(5) Für $b \in \mathfrak{b}$ ist $\mathrm{Tr}_{L|K}((b)) = (\mathrm{Tr}_{L|K}(b))$.

(6) Für $\mathfrak{h} \in \underline{\mathrm{Ideale}}^\times(B)$ und $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ ist $\mathrm{Tr}_{L|K}(\mathfrak{h})_\mathfrak{p} = \mathrm{Tr}_{L|K}(\mathfrak{h}_\mathfrak{p})$.

(7) Es ist $\mathrm{Tr}_{L|K}(B^{\#,A}) = A$.

Aufgabe 38 (§2.3.4) Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt.

Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$.

Sei $L|K$ eine endliche Körpererweiterung. Sei $B = \Gamma_L(A)$.

Zeige.

(1) Es ist $(\mathfrak{D}_{L|K,A})_{\mathfrak{p}} = \mathfrak{D}_{L|K,A_{\mathfrak{p}}}$.

(2) Es ist $(\mathfrak{d}_{L|K,A})_{\mathfrak{p}} = \mathfrak{d}_{L|K,A_{\mathfrak{p}}}$.

Aufgabe 39 (§2.3.4, §1.4.3) Sei A ein Dedekindbereich. Sei $K := \mathrm{Quot}(A)$ perfekt.

Seien $L'|K$ und $L''|K$ linear disjunkte endliche Körpererweiterungen.

Sei L eine gemeinsame Körpererweiterung von L' und L'', welche ein Kompositum von $L'|K$ und $L''|K$ ist.

Schreibe $\ell' := [L' : K]$ und $\ell'' := [L'' : K]$.

Sei $\mathfrak{d}_{L'|K,A} + \mathfrak{d}_{L''|K,A} = (1)$.

Zeige $\mathfrak{d}_{L|K,A} \;=\; \mathfrak{d}^{\ell''}_{L'|K,\,A} \cdot \mathfrak{d}^{\ell'}_{L''|K,A}$.

Aufgabe 40 (§2.3.4, §1.4.3)

Sei $K := \mathbf{Q}$, sei $L := \mathbf{Q}(\sqrt{13})$, sei $L' := \mathbf{Q}(\sqrt{3})$ und sei $M := \mathbf{Q}(\sqrt{3}, \sqrt{13})$. Cf. Aufgabe 16.(2).

Sei $A := \mathbf{Z}$, sei $B := \Gamma_L(A)$, sei $B' := \Gamma_L(A)$ und sei $C := \Gamma_M(A)$.

(1) Bestimme $\mathfrak{D}_{L|K,A}$. Bestimme $\mathfrak{D}_{M|L,B}$. Bestimme damit $\mathfrak{D}_{M|K,A}$.

(2) Bestimme $\mathfrak{D}_{L'|K,A}$. Bestimme $\mathfrak{D}_{M|L',B}$. Bestimme damit $\mathfrak{D}_{M|K,A}$ erneut.

(3) Bestätige die Aussage von Lemma 96 für $L|K$, $L'|K$ und $M|K$ durch Vergleich der Resultate hier mit den Resultaten aus Aufgabe 16.(2).

Aufgabe 41 (§3.1) Sei V ein euklidischer Raum. Zeige.

Für eine Teilmenge $X \subseteq V$ sind die folgenden Aussagen $(1, 2)$ äquivalent.

Für eine additive Untergruppe $X \subseteq V$ sind die folgenden Aussagen $(1, 2, 3, 4)$ äquivalent.

(1) Es ist X eine diskrete Teilmenge von V.

(2) Für alle $v \in V$ gibt es ein $\varepsilon \in \mathbf{R}_{>0}$ mit $(\mathrm{B}_{\varepsilon}(v) \smallsetminus \{v\}) \cap X = \emptyset$.

(3) Es gibt ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\mathrm{B}_{\varepsilon}(0) \cap X = \{0\}$.

(4) Es gibt ein $r \in \mathbf{R}_{>0}$ mit $\mathrm{B}_r(0) \cap X$ endlich.

Aufgabe 42 (§3.2.1) Sei $K|\mathbf{Q}$ eine endliche Körpererweiterung.

Gib die Abbildungen $\mathrm{Tr}\,|^{\mathbf{R}}_{K_{\mathbf{R}}} : K_{\mathbf{R}} \longrightarrow \mathbf{R}$ und $\mathrm{N}\,|^{\mathbf{R}}_{K_{\mathbf{R}}} : K_{\mathbf{R}} \longrightarrow \mathbf{R}$ unter Verwendung von Koeffizienten bezüglich der Orthonormalbasis aus Bemerkung 112 an.

Zeige, daß beide Abbildungen stetig sind.

Aufgabe 43 (§2.3.3, §3.2.2) Sei A ein Dedekindbereich. Sei $K = \mathrm{Quot}(A)$ perfekt. Sei $L|K$ eine endliche Körpererweiterung. Schreibe $\ell := [L : K]$. Sei $B := \Gamma_L(A)$. Sei $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$.

(1) Sei $\mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ mit $\mathfrak{p} \subseteq \mathfrak{q}$. Zeige, daß $\mathfrak{p} = A \cap \mathfrak{q}$ ist und daß $(B/\mathfrak{q})|(A/\mathfrak{p})$ eine endliche Körpererweiterung ist. Sei $f := [B/\mathfrak{q} : A/\mathfrak{p}]$. Zeige $\mathrm{N}_{L|K}(\mathfrak{q}) = \mathfrak{p}^f$.

(2) Sei $\mathfrak{p}B = \prod_{i\in[1,d]} \mathfrak{q}_i^{e_i}$ die Primidealfaktorzerlegung in B, wobei $d \geqslant 1$, wobei $\mathfrak{q}_i \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B)$ und $e_i \geqslant 1$ für $i \in [1,d]$ und wobei $\mathfrak{q}_i \neq \mathfrak{q}_j$ für $i, j \in [1,d]$ mit $i \neq j$; cf. Lemma 54, Satz 63. Schreibe $f_i := [B/\mathfrak{q}_i : A/\mathfrak{p}]$ für $i \in [1,d]$.

Zeige

$$\ell \;=\; \sum_{i\in[1,d]} e_i f_i \;.$$

Hinweis: Berechne $\mathrm{N}_{L|K}(\mathfrak{p}B)$ mit (1) und alternativ mit Aufgabe 34.(3).

(3) Bestätige die Formel aus (2) im Falle $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt[3]{2})$ für $\mathfrak{p} \in \{(3), (5), (7)\}$. Cf. Aufgabe 30.(4).

Aufgabe 44 (§2.3.1, Aufgabe 43) Sei R ein diskreter Bewertungsring mit maximalem Ideal erzeugt von $r \in R$. Sei $K := \mathrm{Quot}(R)$. Sei $L|K$ eine endliche Körpererweiterung. Sei $s \in \Gamma_L(R)^{\times}$ gegeben. Schreibe $S := R[s]$. Schreibe $\mu(X) := \mu_{s,K}(X) \in R[X]$ und $m := \deg \mu$.

(1) Zeige, daß S genau dann ein diskreter Bewertungsring mit maximalem Ideal erzeugt von s ist, wenn $\mu(X)$ *eisensteinsch* ist, i.e. wenn $\mu(X) \equiv_r 0$ und $\mu(0) \not\equiv_{r^2} 0$ ist. Zeige, daß diesenfalls $R/(r)$ und $S/(s)$ isomorphe Ringe sind und daß $(r) = (s^m)$. Hinweis: Betrachte $(R/(r))[X]/X^m \longrightarrow S/(r)$.

(2) Verifiziere (1) am Beispiel $R = \mathbf{Z}_{(p)}$, $r = p$, $s = \zeta_p - 1$.

(3) Verifiziere (1) am Beispiel $R = \mathbf{Z}_{(p)}[\zeta_p]$, $r = \zeta_p - 1$, $s = \zeta_{p^2} - 1$.

Aufgabe 45 (§3.2.2, §3.2.3)

(1) Seien $m, n \in \mathbf{Z}_{\geqslant 0}$. Seien $u_i \in \mathbf{R}_{>0}$ für $i \in [1,n]$; schreibe $u := (u_i)_{i\in[1,n]}$. Seien $v_i \in \mathbf{R}_{>0}$ für $i \in [1,m]$; schreibe $v := (v_i)_{i\in[1,m]}$.

Sei

$$\begin{aligned} Z_{u,v} &:= \{\, (x_1\,,\,\ldots\,,\,x_n\,,\,y_1\,,\,\ldots\,,\,y_m\,,\,z_1\,,\,\ldots\,,\,z_m\,) \in \mathbf{R}^{n+2m} \,: \\ &\qquad\qquad |x_i| \leqslant u_i \text{ für } i \in [1,n],\ 2^{-1/2}(y_i^2+z_i^2)^{1/2} \leqslant v_i \text{ für } i \in [1,m]\,\} \\ &\subseteq \mathbf{R}^{n+2m}\,. \end{aligned}$$

Zeige

$$\mathrm{vol}(Z_{u,v}) \;=\; 2^{n+m}\pi^m(\prod_{i\in[1,n]} u_i)(\prod_{i\in[1,m]} v_i^2)\,.$$

Hinweis: Schreibe $u' := (u_i)_{i\in[1,n-1]}$ und $v' := (v_i)_{i\in[1,m-1]}$. Erstelle Zusammenhang zwischen $Z_{u,v}$, $Z_{u',v}$, $Z_{u,v'}$.

(2) Sei $R \in \mathbf{R}_{\geqslant 0}$. Seien $n,\, m \,\in\, \mathbf{Z}_{\geqslant 0}$. Sei

$$\begin{aligned} M_{n,m,R} &:= \big\{\, (x_1\,,\,\ldots\,,\,x_n\,,\,y_1\,,\,\ldots\,,\,y_m\,,\,z_1\,,\,\ldots\,,\,z_m\,) \in \mathbf{R}^{n+2m} \,: \\ &\qquad\qquad \big(\textstyle\sum_{i\in[1,n]} |x_i|\big) + 2^{1/2}\big(\sum_{i\in[1,m]}(y_i^2+z_i^2)^{1/2}\big) \leqslant R\,\big\} \\ &\subseteq \mathbf{R}^{n+2m}\,. \end{aligned}$$

Zeige

$$\mathrm{vol}(M_{n,m,R}) \;=\; 2^n\pi^m\frac{R^{n+2m}}{(n+2m)!}\,.$$

Hinweis: Erstelle Zusammenhang zwischen $\mathrm{vol}(M_{n,m,R})$ und $\mathrm{vol}(M_{n-1,m,R})$, sowie zwischen $\mathrm{vol}(M_{n,m,R})$ und $\mathrm{vol}(M_{n,m-1,R})$.

Aufgabe 46 (§3.2.2) Sei $m \geqslant 1$. Seien $a_i \in \mathbf{R}_{>0}$ für $i \in [1,m]$.

Zeige

$$\frac{1}{m}\sum_{i\in[1,m]} a_i \;\geqslant\; (\prod_{i\in[1,m]} a_i)^{1/m}\,.$$

Aufgabe 47 (§3.2.2)

(1) Zeige $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})}) \simeq \mathrm{C}_3$.

(2) Zeige $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-47})}) \simeq \mathrm{C}_5$.

Aufgabe 48 (§3.2.2) Ist $\mathbf{Z}[\sqrt[3]{2}]$ ein Hauptidealbereich?

Aufgabe 49 (§3.2.2)

Sei K ein Zahlkörper, o.E. $\mathbf{C}|K|\mathbf{Q}$. Schreibe $k := [K:\mathbf{Q}]$ und $s := |\mathrm{Einb}_{\mathbf{C}}(K)|$.

(1) Zeige $|\Delta_K| \geqslant \big(\frac{\pi}{4}\big)^{2s} \cdot \Big(\frac{k^k}{k!}\Big)^2$.

(2) Für welche Zahlkörper K ist $|\Delta_K| = 1$?

(3) Zeige mit der Stirlingschen Formel $\lim_{n\to\infty} \frac{n!\,\mathrm{e}^n}{n^n\sqrt{n}} = \sqrt{2\pi}$, daß es für jedes $C \in \mathbf{R}_{>0}$ ein $N \in \mathbf{Z}_{\geqslant 1}$ so gibt, daß im Falle $[K : \mathbf{Q}] \geqslant N$ stets $5^{-[K:\mathbf{Q}]}|\Delta_K| > C$ ist.

Aufgabe 50 (§3.2.2, §2.3.3)

Sei A ein Dedekindbereich. Sei $K = \mathrm{Quot}(A)$ perfekt.

Sei $L|K$ eine endliche Körpererweiterung. Schreibe $\ell := [L : K]$. Sei $B := \Gamma_L(A)$.

Zeige.

(1) Es gibt den Gruppenmorphismus $\mathrm{N}_{L|K} : \mathrm{Cl}(B) \longrightarrow \mathrm{Cl}(A)$, $[\mathfrak{h}] \longmapsto [\mathrm{N}_{L|K}(\mathfrak{h})]$.

(2) Es gibt den Gruppenmorphismus $\mathrm{ind}_{L|K} : \mathrm{Cl}(A) \longrightarrow \mathrm{Cl}(B)$, $[\mathfrak{g}] \longmapsto [B\mathfrak{g}]$.

(3) Ist $|\mathrm{Cl}(A)|$ teilerfremd zu ℓ, dann ist die Abbildung $\mathrm{ind}_{L|K}$ aus (2) injektiv und die Abbildung $\mathrm{N}_{L|K}$ aus (1) surjektiv.

Aufgabe 51 (§3.2.2, Aufgabe 50)

(1) Sei A ein Dedekindbereich. Sei $\mathfrak{a} \in \mathrm{Ideale}^\times(A)$.

Sei $m \in \mathbf{Z}_{\geqslant 1}$ und $a \in A^\times$ mit $\mathfrak{a}^m = (a)$ gegeben.

Sei $K := \mathrm{Quot}(A)$. Sei M der Zerfällungskörper von $X^m - a \in K[X]$. Sei $b \in M$ eine Nullstelle von $X^m - a$ in M. Sei $L := K(b) \subseteq M$. Somit ist $M|L|K$. Sei $B := \Gamma_L(A)$.

Zeige, daß $B\mathfrak{a}$ ein Hauptideal in B ist.

(2) Zeige, daß es für jeden Zahlkörper K eine endliche Körpererweiterung $L|K$ so gibt, daß $\mathrm{ind}_{L|K} : \mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}(\mathcal{O}_L)$ das Bild $\mathrm{ind}_{L|K}(\mathrm{Cl}(\mathcal{O}_K)) = \{[(1)]\}$ hat, i.e. daß $\mathrm{ind}_{L|K}$ *trivial* ist; cf. Aufgabe 50.(2).

(3) Sei $K := \mathbf{Q}(\sqrt{-5})$. Finde eine endliche Körpererweiterung $L|K$ so, daß $\mathrm{ind}_{L|K} : \mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}(\mathcal{O}_L)$ trivial ist.

Gib für ein Ideal $\mathfrak{a}$ von $\mathcal{O}_K$, das kein Hauptideal ist, ein $b \in \mathcal{O}_L$ mit $\mathcal{O}_L\mathfrak{a} = (b)$ an.

Aufgabe 52 (§3.2.3)

Sei R ein kommutativer Ring. Sei $M' \xrightarrow{i} M \xrightarrow{r} M''$ eine kurz exakte Sequenz von R-Moduln und R-linearen Abbildungen, i.e. sei i injektiv, r surjektiv und sei $i(M) = \mathrm{Kern}(r)$.

Zeige.

(1) Existiere eine R-lineare Abbildung $M \xleftarrow{s} M''$ mit $r \circ s = \mathrm{id}_{M''}$. Dann gibt es eine R-lineare Abbildung $M' \xleftarrow{t} M$ mit $t \circ i = \mathrm{id}_{M'}$, und es ist $M \simeq M' \oplus M''$.

(2) Sei $M'' \simeq R^{\oplus n}$ für ein $n \in \mathbf{Z}_{\geqslant 0}$. Dann gibt es einen R-linearen Isomorphismus $M \xleftarrow{\sim} M' \oplus M''$, der $m' \in M'$ auf $i(m')$ schickt.

Aufgabe 53 (§3.2.3)

Sei $d \in \mathbf{Z}_{\geqslant 2}$ quadratfrei.

(1) Zeige, daß es genau ein $u \in \mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})}) \cap \mathbf{R}_{>1}$ so gibt, daß für alle $v \in \mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})})$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u^m, +u^m\}$ existiert.

(2) Bestimme u wie in (1) für $d \in \{2, 3, 5, 17, 19\}$.

Aufgabe 54 (§3.2.3)

Sei K ein Zahlkörper mit $[K : \mathbf{Q}] = 3$, mit $K \subseteq \mathbf{R}$, mit $\mathrm{Einb}_{\mathbf{R}}(K) =: \{\iota\}$
und mit $\mathrm{Einb}_{\mathbf{C}}(K) =: \{\sigma\}$.

Zeige.

(1) Sei $v \in \mathrm{U}(\mathcal{O}_K) \cap \mathbf{R}_{>1}$. Dann ist $\mathrm{N}_{K|\mathbf{Q}}(v) = +1$. Mit $x := \sqrt{v}$ und einem geeigneten $t \in \mathbf{R}$ können wir $\sigma(v) = x^{-1} \exp(\mathrm{i}t)$ schreiben.

(2) Sei $v \in \mathrm{U}(\mathcal{O}_K) \cap \mathbf{R}_{>1}$. Dann ist $|\Delta_K| \leqslant |\Delta_{K|\mathbf{Q},\,(1,v,v^2)}| < 4v^3 + 24$.

(3) Sei $u \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < u$ und $4u^{3/2} + 24 \leqslant |\Delta_K|$ gegeben. Dann gibt es für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u^m, +u^m\}$.

(4) Sei $K := \mathbf{Q}(\sqrt[3]{2})$. Es gibt genau ein $u \in \mathrm{U}(\mathcal{O}_K)$ mit $u > 1$ und derart, daß für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u^m, +u^m\}$ existiert. Bestimme u.

(5) Es ist $f(X) := X^3 + 2X + 1 \in \mathbf{Q}[X]$ irreduzibel. Es hat $f(X)$ genau eine reelle Nullstelle α. Sei $K := \mathbf{Q}(\alpha)$. Es gibt genau ein $u \in \mathrm{U}(\mathcal{O}_K)$ mit $u > 1$ und derart, daß für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u^m, +u^m\}$ existiert. Bestimme u.

Aufgabe 55 (§3.2.2, §4.1)

Zeige mittels Minkowskitheorie, daß $\mathbf{Z}[\zeta_n]$ ein Hauptidealbereich ist für $n \in \{3, 4, 5, 7, 8\}$.

Für $n \in \{3, 4\}$ wissen wir dies bereits aus Aufgabe 6.(3, 2).

Aufgabe 56 (§3.2.3, §4.1)

Bestimme alle Einheiten in $\mathbf{Z}[\zeta_5]$.

Hinweis: Wir haben einen Gruppenmorphismus $\mathrm{U}(\mathbf{Z}[\zeta_5]) \longrightarrow \mathrm{U}(\mathcal{O}_{\mathbf{Q}(\zeta_5)\cap\mathbf{R}})$; cf. Aufgabe 53.(2).

Aufgabe 57 (§4.1)

Sei $p \in \mathbf{Z}_{>0}$ eine Primzahl. Sei $\alpha \in \mathbf{Z}_{\geqslant 1}$.

Bestimme $\Delta_{\mathbf{Q}(\zeta_{p^\alpha})}$.

Hinweis: Wie in Lemma 129.(4), nur unter Beachtung des Vorzeichens.

Aufgabe 58 (Aufgabe 59)

Sei $p \in \mathbf{Z}_{\geqslant 3}$ prim. Sei a, $b \in \mathbf{Z} \smallsetminus (p)$. Sei $a^* \in \mathbf{Z}$ mit $aa^* \equiv_p 1$ gegeben.

Das *Legendresymbol* ist gegeben durch

$$\left(\tfrac{a}{p}\right) := \begin{cases} +1 & \text{falls } a+(p) \in (\mathbf{F}_p^\times)^2 \\ -1 & \text{falls } a+(p) \notin (\mathbf{F}_p^\times)^2 \,. \end{cases}$$

Sei $\tau := \sum_{a+(p) \in \mathrm{U}(\mathbf{Z}/(p))} \left(\tfrac{a}{p}\right) \zeta_p^a$.

(1) Zeige $\left(\tfrac{a}{p}\right) \equiv_p a^{(p-1)/2}$, $\left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) = \left(\tfrac{ab}{p}\right)$ und $\left(\tfrac{a}{p}\right) = \left(\tfrac{a^*}{p}\right)$.

(2) Zeige $\tau^2 = \left(\tfrac{-1}{p}\right)p$.

(3) Zeige, daß $\mathbf{Q}(\sqrt{\left(\tfrac{-1}{p}\right)p})$ ein Teilkörper von $\mathbf{Q}(\zeta_p)$ ist.

Aufgabe 59 (§2.2, §4.1, Aufgabe 55)

(1) Zeige, daß $\mathbf{Q}(\sqrt{-23})$ ein Teilkörper von $\mathbf{Q}(\zeta_{23})$ ist.

(2) Ist $\mathbf{Z}[\zeta_{23}]$ ein Hauptidealbereich?

Hinweis: Aufgabe 50 verwenden, um $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})}) \simeq \mathrm{C}_3$ aus Aufgabe 47.(1) zum Einsatz bringen zu können.

Aufgabe 60 (§4.1)

(1) Bestimme $\Delta_{\mathbf{Q}(\zeta_{40})}$.

(2) Bestimme die Primidealfaktorzerlegungen in $\mathbf{Z}[\zeta_{40}]$ von (2), (3) und (5).

(3) Für welche Primzahlen p ist das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_p[X]$ irreduzibel? Für welche zerfällt es in Linearfaktoren?

Aufgabe 61 (§4.2.2, §4.2.1)

Sei $L|\mathbf{Q}$ eine endliche galoische Körpererweiterung mit nichtzyklischer Galoisgruppe.

Sei $\mathcal{O}_L$ als Ring von einem Element erzeugt.

Zeige :

Es gibt nur endlich viele $p \in \mathbf{Z}_{>0}$ prim derart, daß (p) bezüglich $K|\mathbf{Q}$ Zerlegungsbreite 1 hat.

Aufgabe 62 (§4.2.2, §2.3.4)

Schreibe $\delta := \sqrt[3]{2}$ und $\zeta := \zeta_3$. Sei $L := \mathbf{Q}(\delta, \zeta)$. Sei $K := \mathbf{Q}$.

(1) Bestimme $\mathcal{O}_L$. Bestimme $|\Delta_L|$ unter Verwendung von Satz 100.(2).

Hinweis: Nach Aufgabe 19.(2) ist $\mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$. Verwende $\Delta_{\mathbf{Q}(\zeta,\delta)|\mathbf{Q}(\delta),\,(1,\eta)}$ mit $\eta \in \mathcal{O}_L$ geeignet. Cf. Aufgabe 18.(3).

(2) Bestimme die Primidealfaktorzerlegung von (5) in $\mathcal{O}_L$. Gib die Zerlegungsparameter von (5) an. Welcher dieser Zerlegungsparameter ist bereits aus (1) bekannt?

Hinweis: Bestimme zunächst die Primidealfaktorzerlegung von (5) in $\mathbf{Z}[\delta]$.

(3) Wähle ein Primideal $\mathfrak{q}$ von $\mathcal{O}_L$, welches (5) enthält. Bestimme seinen Zerlegungskörper L_{dec} und seinen Trägheitskörper L_{inert} .

(4) Zeige oder widerlege jeweils.

In der Situation von Satz 143 sei $\mathfrak{r} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(B_{\mathrm{dec}}) \smallsetminus \{\mathfrak{q}_{\mathrm{dec}}\}$ mit $\mathfrak{r} \supseteq \mathfrak{p}$ gegeben. Dann ist der Trägheitsindex von $\mathfrak{r}$ bezüglich $L_{\mathrm{dec}}|K$ gleich 1. Ferner ist die Zerlegungsbreite von $\mathfrak{p}$ bezüglich $L_{\mathrm{dec}}|K$ ist gleich der Zerlegungsbreite von $\mathfrak{p}$ bezüglich $L|K$.

Aufgabe 63 (§4.2.2) Schreibe $\zeta := \zeta_{24}$. Betrachte $\mathbf{Q}(\zeta)|\mathbf{Q}$. Schreibe $B := \mathbf{Z}[\zeta]$.

(1) Sei $\mathfrak{q}$ ein Primideal von B, das 3 enthält. Bestimme Zerlegungskörper und Trägheitskörper von $\mathfrak{q}$. Wieso hängen beide nicht von der Wahl von $\mathfrak{q}$ ab?

(2) Bestimme die Primidealfaktorisierung von (3) in B_{dec} . Vergleiche mit Satz 143.(1).

(3) Bestimme die Primidealfaktorisierung von $B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}}$. Vergleiche mit Satz 143.(2).

(4) Bestimme die Primidealfaktorisierung von $B\mathfrak{q}_{\mathrm{inert}}$. Vergleiche mit Satz 143.(3).

Aufgabe 64 (Aufgabe 58)

Seien p und ℓ zwei verschiedene Primzahlen in $\mathbf{Z}_{\geqslant 3}$.

Zeige $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}$.

Hinweis: Berechne τ^ℓ aus Aufgabe 58 modulo ℓ auf zwei Arten, einmal mittels Aufgabe 58, einmal mittels Frobenius.

Diese Gleichung ist das *Gaußsche Reziprozitätsgesetz.*

A.2 Lösungen

Aufgabe 1

Ad (1). Betrachte den Polynomring $S := \mathbf{Z}[X_r \,:\, r \in R]$. Dies ist ein Integritätsbereich, da jede Ausführung der Multiplikation einen endlichen Träger hat und da von Polynomringen in endlich vielen Variablen bekannt ist, daß sie nullteilerfrei sind.

Setze

$$\begin{array}{rcl} S & \xrightarrow{\varphi} & R \\ X_r & \longmapsto & r \end{array}$$

Dies definiert einen Ringmorphismus; cf. **[5,** §1.6.2], wobei noch Polynomringe in unendlich vielen Variablen zuzulassen sind.

Man kann auch die Abbildungsvorschrift von φ insgesamt angeben. Sei I die Menge der Tupel $\alpha = (\alpha_r)_{r\in R}$ mit $\alpha_r \in \mathbf{Z}_{\geqslant 0}$, für die der Träger $\{\, r \in R \,:\, \alpha_r \neq 0 \,\}$ endlich ist.

Ist

$$f \;=\; \sum_{\alpha\in I} z_\alpha \prod_{r\in R} X_r^{\alpha_r} \;,$$

wobei $\{\, \alpha \in I \,:\, z_\alpha \neq 0 \,\}$ endlich sei, dann ist

$$\varphi(f) \;=\; \sum_{\alpha\in I} z_\alpha \prod_{r\in R} r^{\alpha_r} \;.$$

Es ist φ surjektiv, da für $r \in R$ ja X_r auf r abgebildet wird.

> Man kann sich auch auf freie Erzeuger X_r eines Polynomrings beschränken, für die r nur gewisse Ringerzeuger von R durchläuft.

Ad (2). Sei $\varphi : S \to R$ ein surjektiver Ringmorphismus mit S Integritätsbereich; cf. (1). Sei $K = \mathrm{Quot}(S)$. Es ist also $S \subseteq K$ ein Teilring.

Sei $n \geqslant 0$. Wir schreiben die eintragsweise Anwendung von φ als

$$\begin{array}{rcl} S^{n\times n} & \xrightarrow{\hat\varphi} & R^{n\times n} \\ (s_{i,\,j})_{i,\,j} & \longmapsto & \hat\varphi((s_{i,\,j})_{i,\,j}) \;:=\; (\varphi(s_{i,\,j}))_{i,\,j} \;. \end{array}$$

Es ist $\hat\varphi$ ein Ringmorphismus.

Sei $A = (a_{i,\,j})_{i,\,j} \in R^{n\times n}$ gegeben.

Sei $A' = (a'_{u,v})_{u,v} \in R^{n\times n}$ definiert durch

$$a'_{v,u} \;=\; (-1)^{u+v} \det((a_{i,\,j})_{i\in[1,n]\smallsetminus\{v\},\; j\in[1,n]\smallsetminus\{u\}})$$

für $u,\, v \in [1,n]$. Wir haben $A'A \stackrel{!}{=} \det(A)\mathrm{E}_n$ zu zeigen.

Wähle $b_{i,\,j} \in S$ mit $\varphi(b_{i,\,j}) = a_{i,\,j}$ für $i,\, j \in [1,n]$. Setze $B := (b_{i,\,j})_{i,\,j} \in S^{n\times n} \subseteq K^{n\times n}$. Es ist also $\hat\varphi(B) = A$. Es ist ferner

$$\det(A) \;=\; \det(\hat\varphi(B)) \;=\; \det(\varphi(b_{i,\,j}))_{i,\,j} \;=\; \varphi(\det(b_{i,\,j})_{i,\,j}) \;=\; \varphi(\det(B)) \;,$$

da die Determinante ein polynomialer Ausdruck in den Matrixeinträgen mit Koeffizienten in $\{-1,+1\}$ ist.

Sei $B' = (b'_{u,v})_{u,v} \in S^{n\times n} \subseteq K^{n\times n}$ definiert durch

$$b'_{v,u} \;=\; (-1)^{u+v} \det((b_{i,\,j})_{i\in[1,n]\smallsetminus\{v\},\; j\in[1,n]\smallsetminus\{u\}})$$

für $u,\, v \in [1,n]$. Nach Cramerscher Regel über K ist $B'B = \det(B)\mathrm{E}_n$.

Es ist

$$\begin{aligned}\varphi(b'_{v,u}) &= \varphi\big((-1)^{u+v} \det((b_{i,\,j})_{i\in[1,n]\smallsetminus\{v\},\; j\in[1,n]\smallsetminus\{u\}})\big)\\ &= (-1)^{u+v} \det((\varphi(b_{i,\,j}))_{i\in[1,n]\smallsetminus\{v\},\; j\in[1,n]\smallsetminus\{u\}}\\ &= (-1)^{u+v} \det((a_{i,\,j})_{i\in[1,n]\smallsetminus\{v\},\; j\in[1,n]\smallsetminus\{u\}}\end{aligned}$$

für $u,\, v \in [1,n]$.

Zusammengenommen ist also $\hat\varphi(B') = A'$.

Somit wird in der Tat

$$A'A \;=\; \hat\varphi(B')\hat\varphi(B) \;=\; \hat\varphi(B'B) \;=\; \hat\varphi(\det(B)\mathrm{E}_n) \;=\; \varphi(\det(B))\mathrm{E}_n \;=\; \det(A)\mathrm{E}_n\;.$$

Aufgabe 2

Ad (1). *Annahme,* nicht. Dann können wir, ausgehend von einem Ideal in M, eine strikt aufsteigende Kette von Idealen $I_1 \subset I_2 \subset \ldots$ bilden. Es ist $I := \bigcup_{k\geqslant 1} I_k$ ein Ideal in R, da $0 \in I$ und da für $x,\, x' \in I$ und $r,\, r' \in R$ es ein $m \geqslant 1$ gibt mit $x,\, x' \in I_m$, sodaß auch $rx + r'x' \in I_m \subseteq I$ liegt. Da R ein Hauptidealbereich ist, gibt es ein $a \in R$ mit $I = (a)$. Nun gibt es auch ein $n \geqslant 1$ mit $a \in I_n$. Folglich ist $I_n \subseteq I = (a) \subseteq I_n$, und also $I = I_n \subset I_{n+1} \subseteq I$, *Widerspruch.*

Ad (2). Sei $a \in R^\times$ gegeben.

Sei $a \in R$ prim. Dann folgt aus $a = bc$, daß $(b+(a))(c+(a)) = 0$ ist in $R/(a)$, also o.E. $b+(a) = 0$ und somit $b = ad$ für ein $d \in R$ ist. Dann aber ist $a = bc = adc$ und somit $1 = dc$, also $c \in \mathrm{U}(R)$. Ferner ist $R/(a)$ als Integritätsbereich nicht der Nullring, und somit $(a) \neq R$. Dies zeigt, daß a irreduzibel ist.

Sei $a \in R$ irreduzibel. Zunächst ist $(a) \neq R$ und also $R/(a)$ nicht der Nullring.

Seien $b,\, c \in R$ gegeben mit $(b+(a))(c+(a)) = 0$ in $R/(a)$. Dann gibt es ein $d \in R$ mit $bc = da$. Ist $b+(a) = 0$, so sind wir fertig. Ist $b+(a) \neq 0$, so haben wir $c+(a) \overset{!}{=} 0$ zu zeigen. Es ist $(a) \subset (a,b)$, da $b \notin (a)$. Da R ein Hauptidealbereich ist, gibt es ein $e \in R$ mit $(a,b) = (e)$. Also ist $a = ex$ für ein $x \in R$. Da a irreduzibel ist, folgt $(e) = R$ oder $(x) = R$. *Annahme* $(x) = R$. Dann gibt es ein $y \in R$ mit $xy = 1$, und es wird $e = exy = ay \in (a)$, also $(e) = (a) \subset (a,b) = (e)$, *Widerspruch.* Folglich ist $(e) = R$. Also ist $1 \in (e) = (a,b)$, i.e. es gibt $s,\, t \in R$ mit $1 = sa + tb$. Es folgt $c = sac + tbc = sac + tda = (sc+td)a \in (a)$, i.e. $c + (a) = 0$.

Ad (3). Betrachte die Menge M aller Ideale der Form (x) mit $x \in R^\times$ ohne Primfaktorzerlegung. *Annahme,* es ist $M = \emptyset$. Dank (1) gibt es ein $y \in R$ mit (y) maximal in M.

Es kann y nicht irreduzibel sein, denn sonst hätte $y \in R$ eine Primfaktorzerlegung mit einem Faktor; cf. (2). Also gibt es $b,\, c \in R$ mit $y = bc$ und $b,\, c \notin \mathrm{U}(R)$.

Also ist $y \in (b)$, aber nicht $b \in (y)$, da letzteres $b = dy$ für ein $d \in R$, also $y = bc = cdy$, mithin $1 = cd$ und somit $c \in \mathrm{U}(R)$ nach sich zöge.

Folglich ist $(y) \subset (b)$. Genauso ist $(y) \subset (c)$. Also sind $(b),\, (c) \notin M$. Somit haben b und c je eine Primfaktorzerlegung. Also hat auch $y = bc$ eine Primfaktorzerlegung.

Seien nun mit $(p_1)(p_2)\cdots(p_n) = (p'_1)(p'_2)\cdots(p'_{n'})$ zwei Primfaktorzerlegungen desselben Elements gegeben. Wir führen eine Induktion nach $n \geqslant 0$.

Im Falle $n = 0$ ist auch $n' = 0$, da die auf der rechten Seite auftretenden Primelemente keine Einheiten sind.

Sei nun $n \geqslant 1$. Da p_n prim ist und da das Bild der rechten Seite in $R/(p_n)$ verschwindet, gibt es ein $i \in [1, n']$ und ein $e \in R$ mit $p'_i = ep_n$. O.E. ist $i = n'$. Da $p'_{n'}$ irreduzibel und p_n keine Einheit ist, ist e eine Einheit. Es folgt aus

$$p_1 p_2 \cdots p_{n-1} p_n \;=\; p'_1 p'_2 \cdots p'_{n'-1} p'_{n'} \;=\; p'_1 p'_2 \cdots p'_{n'-1} p_n e \,,$$

daß

$$p_1 p_2 \cdots p_{n-1} \;=\; p'_1 p'_2 \cdots p'_{n'-1} e \,,$$

ist, mithin

$$(p_1)(p_2) \cdots (p_{n-1}) \;=\; (p'_1)(p'_2) \cdots (p'_{n'-1}) \,.$$

Dank Induktion ist nun $n - 1 = n' - 1$, i.e. $n = n'$, und es gibt ein $\tilde{\sigma} \in \mathrm{S}_{n-1}$ mit $(p'_i) = (p_{\tilde{\sigma}(i)})$ für $i \in [1, n-1]$. Sei $\sigma \in \mathrm{S}_n$ durch $\sigma|_{[1,n-1]}^{[1,n-1]} = \sigma$ und $\sigma(n) = n$ festgelegt. Dann ist $(p'_i) = (p_{\sigma(i)})$ für $i \in [1, n]$.

Ad (4). Schreibe $x = \frac{a}{b}$ mit a, $b \in R^\times$. Mit (3) finden wir $k \geqslant 0$ und Primelemente p_i aus $R^\times$ für $i \in [1, k]$ so, daß wir

$$\begin{array}{rcl} a & = & s \prod_{i \in [1,k]} p_i^{\alpha_i} \\ b & = & t \prod_{i \in [1,k]} p_i^{\beta_i} \end{array}$$

mit s, $t \in \mathrm{U}(R)$ und $\alpha_i \,, \beta_i \in \mathbf{Z}_{\geqslant 0}$ schreiben können, wobei $(p_i) \neq (p_j)$ ist für i, $j \in [1, k]$ mit $i \neq j$.

Dank der Eindeutigkeitsaussage aus (3) hängen die Exponenten α_i nicht von der Wahl der p_i ab.

Wir setzen

$$\mathrm{v}_p(x) \;:=\; \begin{cases} \alpha_i - \beta_i & \text{falls } (p) = (p_i) \text{ für ein } i \in [1, k] \\ 0 & \textit{sonst} \end{cases}$$

Mit $e := st^{-1}$ ist dann $x = e \prod_{(p) \in P} p^{\mathrm{v}_p(x)}$.

Bleibt zu zeigen, daß $\mathrm{v}_p(x)$ wohldefiniert ist, i.e. nicht von der Wahl von a und b abhängt.

Sei $x = \frac{a}{b} = \frac{a'}{b'}$ mit a, b, a', $b' \in R^\times$. Wir können nun

$$\begin{array}{rcl} a & = & s \prod_{i \in [1,k]} p_i^{\alpha_i} \\ b & = & t \prod_{i \in [1,k]} p_i^{\beta_i} \\ a' & = & s' \prod_{i \in [1,k]} p_i^{\alpha'_i} \\ b' & = & t' \prod_{i \in [1,k]} p_i^{\beta'_i} \end{array}$$

mit s, t, s', $t' \in \mathrm{U}(R)$ und $\alpha_i \,, \beta_i \,, \alpha_i \,, \beta_i \in \mathbf{Z}_{\geqslant 0}$ schreiben, wobei $(p_i) \neq (p_j)$ ist für i, $j \in [1, k]$ mit $i \neq j$.

Es ist $ab' = a'b$, und also

$$st' \prod_{i \in [1,k]} p_i^{\alpha_i + \beta'_i} \;=\; s't \prod_{i \in [1,k]} p_i^{\alpha'_i + \beta_i}$$

Dank der Eindeutigkeitsaussage aus (3) ist nun $\alpha_i + \beta'_i = \alpha'_i + \beta_i$ für $i \in [1, k]$. Es folgt $\alpha_i - \beta_i = \alpha'_i - \beta'_i$ für $i \in [1, k]$.

Ad (5). Ist $x = 0$ oder $y = 0$, so folgen die Aussagen aus den Regeln für ∞ aus (4).

Sei nun x, $y \in K^\times$.

Es ist $\mathrm{v}_p(xy) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$ wegen der definierenden Charakterisierung der Bewertungen aus (4).

Zur zweiten Zeile. Sei o.E. $\mathrm{v}_p(x) \leqslant \mathrm{v}_p(y)$. Wir haben $\mathrm{v}_p(x + y) \overset{!}{\geqslant} \mathrm{v}_p(x)$ zu zeigen.

Nach der definierenden Charakterisierung der Bewertungen aus (4) gibt es ein $z \in K^\times$ mit $\mathrm{v}_p(zx) = 0$ und zx, $zy \in R^\times$. Es folgt

$$\mathrm{v}_p(x + y) - \mathrm{v}_p(x) \;=\; \mathrm{v}_p(x + y) + \mathrm{v}_p(z) \;=\; \mathrm{v}_p((x + y)z) \;=\; \mathrm{v}_p(zx + zy) \;\geqslant\; 0 \,.$$

Ist nun $\mathrm{v}_p(x) < \mathrm{v}_p(y)$, so ist $\mathrm{v}_p(x+y) \stackrel{!}{=} \mathrm{v}_p(x)$ zu zeigen. Diesenfalls ist in voriger Rechnung $\mathrm{v}_p(zy) > 0$, also $zy = pr$ für ein $r \in R$. *Wäre* $zx + zy$ in R durch p teilbar, dann auch $(zx + zy) - pr = zx$, was *nicht* der Fall ist. Also ist in voriger Rechnung das $\geqslant$ eine Gleichheit.

Ad (6).

Ad (i). Es ist 1 ein p-ganzes Element, da $\mathrm{v}_p(1) = 0$.

Es ist das Produkt zweier p-ganzer Elemente $x, y \in K$ wiederum p-ganz, da $\mathrm{v}_p(xy) = \mathrm{v}_p(x) + \mathrm{v}_p(y) \geqslant 0$ mit (5).

Es ist die Summe zweier p-ganzer Elemente $x, y \in K$ wiederum p-ganz, da sich $\mathrm{v}_p(x+y) \geqslant \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} \geqslant 0$ ergibt mit (5).

Ad (ii). Sei o.E. $z \in K^\times$.

Ist $z \in R^\times$, so ist z ein q-ganzes Element für alle $q \in R^\times$ prim dank (3).

Ist z ein q-ganzes Element für alle $q \in R^\times$ prim, dann zeigt die definierende Charakterisierung der Bewertungen aus (4), daß $z \in R$ liegt.

Ad (7).

Schreibe $g(X) = \sum_{i\in[0,k]} g_i X^i$ mit $k \geqslant 0$, $g_i \in K$ für $i \in [0,k]$ und $g_k = 1$. Setze noch $g_i := 0$ für $i > k$.

Schreibe $h(X) = \sum_{j\in[0,\ell]} h_j X^j$ mit $\ell \geqslant 0$, $h_j \in K$ für $j \in [0,\ell]$ und $h_\ell = 1$. Setze noch $h_j := 0$ für $j > \ell$.

Nach Voraussetzung ist für $m \geqslant 0$ der Koeffizient $f_m := \sum_{i\in[0,m]} g_i h_{m-i}$ von X^m in $f(X) = g(X)h(X)$ ein Element von R.

Annahme, es ist $g(X) \notin R[X]$. Dann können wir ein $p \in R^\times$ prim so wählen, daß

$$\alpha \;:=\; \min\{\, \mathrm{v}_p(g_i) \,:\, i \in [0,k] \,\} \;<\; 0$$

ist. Sei $s \in [0,k]$ maximal mit $\mathrm{v}_p(g_s) = \alpha$.

Sei ferner $\beta := \min\{\, \mathrm{v}_p(h_j) \,:\, j \in [0,\ell] \,\}$. Da $h_\ell = 1$, ist $\beta \leqslant 0$. Sei $t \in [0,\ell]$ maximal mit $\mathrm{v}_p(h_t) = \beta$.

Nun ist

$$f_{s+t} \;=\; \sum_{i\in[0,s+t]} g_i h_{s+t-i} \;=\; g_s h_t + \Big(\sum_{i\in[0,s-1]} g_i h_{s+t-i}\Big) + \Big(\sum_{i\in[s+1,s+t]} g_i h_{s+t-i}\Big)\,.$$

Es ist $\mathrm{v}_p(g_s h_t) = \alpha + \beta$.

Für $i \in [0, s-1]$ ist $\mathrm{v}_p(g_i h_{s+t-i}) = \mathrm{v}_p(g_i) + \mathrm{v}_p(h_{s+t-i}) \geqslant \alpha + (\beta + 1)$.

Für $i \in [s+1, s+t]$ ist $\mathrm{v}_p(g_i h_{s+t-i}) = \mathrm{v}_p(g_i) + \mathrm{v}_p(h_{s+t-i}) \geqslant (\alpha + 1) + \beta$.

Gemäß (5) folgt $\mathrm{v}_p(f_m) = \mathrm{v}_p(g_s h_t) = \alpha + \beta < 0$, im *Widerspruch* zu $f_m \in R$.

Dito ist $h(X) \in R[X]$.

Aussage (7) heißt auch Lemma von Gauß.

Ad (8).

Ist $\mu_{y,K}(X) \in A[X]$, so ist $\mu_{y,K}(X)$ ein normiertes Polynom in $A[X]$ mit $\mu_{y,K}(y) = 0$. Also ist $y \in \Gamma_L(A) = B$.

Ist umgekehrt $y \in B = \Gamma_L(A)$, dann gibt es ein normiertes Polynom $f(X) \in A[X]$ mit $f(y) = 0$. Es ist $\mu_{y,K}(X)$ ein Teiler von $f(X)$ in $K[X]$, i.e. es gibt $g(X) \in K[X]$ mit $\mu_{y,K}(X)g(X) = f(X)$; cf. **[5,** §2.3]. Da $f(X)$ und $\mu_{y,K}(X)$ normiert sind, ist auch $g(X)$ normiert. Dank (7) ist also $\mu_{y,K}(X) \in A[X]$.

Aufgabe 3

Zunächst merken wir an, daß $\sqrt{d} \in \mathcal{O}_K$ und daher $\mathbf{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$ ist. Es stellt sich die Frage, ob es Elemente in $\mathcal{O}_K$ gibt, die nicht bereits in $\mathbf{Z}[\sqrt{d}]$ liegen.

Es ist $\mathrm{Gal}(K|\mathbf{Q})$ erzeugt von $\sigma : \sqrt{d} \mapsto -\sqrt{d}$.

Sei $w =: a + b\sqrt{d} \in K$ gegeben, wobei a, $b \in \mathbf{Q}$.

Ist $b = 0$, dann wird

$$\mu_{w,\mathbf{Q}}(X) \;=\; X - a \;.$$

Es ist $w \in \mathcal{O}_K$ genau dann, wenn $\mu_{w,\mathbf{Q}}(X) \in \mathbf{Z}[X]$ ist, i.e. wenn $a \in \mathbf{Z}$ liegt. Dann aber ist auch $w \in \mathbf{Z}[\sqrt{d}]$.

Sei von nun an $b \neq 0$. Es wird

$$\mu_{w,\mathbf{Q}}(X) \;=\; (X - a - b\sqrt{d})(X - a + b\sqrt{d}) \;=\; X^2 - 2aX + (a^2 - db^2) \;;$$

cf. Lemma 14. Es ist $w \in \mathcal{O}_K$ genau dann, wenn $\mu_{w,\mathbf{Q}}(X) \in \mathbf{Z}[X]$ ist, i.e. wenn $2a \in \mathbf{Z}$ und $a^2 - db^2 \in \mathbf{Z}$ liegen; cf. Aufgabe 2.(8).

Wir haben also nur die Elemente der Form $a + b\sqrt{d}$ mit $a \in \frac{1}{2}\mathbf{Z}$ und $b \in \mathbf{Q}$ daraufhin zu untersuchen, wann sie in $\mathcal{O}_K$ liegen.

Schreibe $a =: x/2$ mit $x \in \mathbf{Z}$.

Es ist w genau dann ganz über $\mathbf{Z}$, wenn $4\mathbf{Z} \ni 4a^2 - 4db^2 = x^2 - 4db^2$ ist. Notwendig dafür ist also $d(2b)^2 \in \mathbf{Z}$. Da d quadratfrei ist, folgt $2b \in \mathbf{Z}$ als notwendige Bedingung.

Wir haben also nur die Elemente der Form $a + b\sqrt{d}$ mit a, $b \in \frac{1}{2}\mathbf{Z}$ daraufhin zu untersuchen, wann sie in $\mathcal{O}_K$ liegen.

Schreibe $b =: y/2$ mit $y \in \mathbf{Z}$.

Es sollte $4(a^2 - db^2) \in 4\mathbf{Z}$, i.e. $x^2 \equiv_4 dy^2$ sein.

Fall $x \equiv_2 0$. Da $d \not\equiv_4 0$, folgt $y \equiv_2 0$. Dann ist $x^2 \equiv_4 0 \equiv_4 dy^2$ erfüllt. Aber diesenfalls ist ohnehin $a + b\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$.

Fall $x \equiv_2 1$. Dann ist $x^2 \equiv_4 1$. Also ist $y \equiv_2 1$.

Unterfall $d \equiv_4 1$. Es ist $x^2 \equiv_4 1$ und $dy^2 \equiv_4 1$, also in der Tat $x^2 \equiv_4 dy^2$. Somit ist diesenfalls $a + b\sqrt{d} = \frac{1}{2}(x + y\sqrt{d}) \in \mathcal{O}_K$.

Unterfall $d \equiv_4 2$ *oder* $d \equiv_4 3$. Es ist $x^2 \equiv_4 1$, aber $dy^2 \equiv_4 d \not\equiv_4 1$. Diesenfalls ist also $a + b\sqrt{d} = \frac{1}{2}(x + y\sqrt{d}) \notin \mathcal{O}_K$.

Fassen wir zusammen.

Fall $d \equiv_4 1$. Es ist $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}] \cup \{\, \frac{1}{2}(x + y\sqrt{d}) \,:\, x,\, y \,\in\, 2\mathbf{Z} + 1 \,\}$. Also ist $\frac{1}{2}(1 + \sqrt{d}) \in \mathcal{O}_K$ und damit $\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathcal{O}_K$.

Es ist $\sqrt{d} = 2(\frac{1+\sqrt{d}}{2}) - 1 \in \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, und also $\mathbf{Z}[\sqrt{d}] \subseteq \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. Daher ist für x, $y \in 2\mathbf{Z} + 1$ auch $\frac{1}{2}(x + y\sqrt{d}) = \frac{1}{2}(1 + \sqrt{d}) + \frac{1}{2}((x-1) + (y-1)\sqrt{d}) \in \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. Dies zeigt $\mathbf{Z}[\frac{1+\sqrt{d}}{2}] \supseteq \mathcal{O}_K$.

Zusammengenommen ist diesenfalls somit $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.

Fall $d \equiv_4 2$ *oder* $d \equiv_4 3$. Es ist $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$.

Speziell erhalten wird die folgenden Ringe ganzer Zahlen.

Es wird $\mathcal{O}_{\mathbf{Q}(\mathrm{i})} = \mathcal{O}_{\mathbf{Q}(\sqrt{-1})} = \mathbf{Z}[\sqrt{-1}] = \mathbf{Z}[\mathrm{i}]$.

Es wird $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\frac{1+\sqrt{5}}{2}]$.

Es wird $\mathcal{O}_{\mathbf{Q}(\zeta_3)} = \mathcal{O}_{\mathbf{Q}(\sqrt{-3})} = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbf{Z}[-\zeta_3^2] = \mathbf{Z}[\zeta_3^2] = \mathbf{Z}[\zeta_3]$, beachte $(\zeta_3^2)^2 = \zeta_3$.

Aufgabe 4

Schreibe $d = d(T)$.

Es ist $\sqrt{d} \in \Gamma_{\mathcal{Q}(\sqrt{d})}(\mathcal{Z})$ und also $\mathcal{Z}[\sqrt{d}] \subseteq \Gamma_{\mathcal{Q}(\sqrt{d})}(\mathcal{Z})$; cf. Lemma 5.

Wir *behaupten* $\mathcal{Z}[\sqrt{d}] \overset{!}{\supseteq} \Gamma_{\mathcal{Q}(\sqrt{d})}(\mathcal{Z})$.

Sei $\xi = a + b\sqrt{d} \in \Gamma_{\mathcal{Q}(\sqrt{d})}(\mathcal{Z})$, wobei $a = a(T)$ und $b = b(T)$ aus $\mathcal{Q}$ stammen.

Ist $b = 0$, dann hat $\xi = a$ Minimalpolynom $\mu_{\xi,\mathcal{Q}}(X) = X - a \overset{\text{A. 2.(8)}}{\in} \mathcal{Z}[X]$, woraus $a \in \mathcal{Z}$ folgt.

Ist $b \neq 0$, dann ist

$$\mu_{\xi,\mathcal{Q}}(T) \;=\; (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) \;=\; T^2 - 2aT + (a^2 - db^2) \overset{\text{A. 2.(8)}}{\in} \mathcal{Z}[X] \,.$$

Aus $2a \in \mathcal{Z}$ folgt wegen $p \neq 2$, daß $a \in \mathcal{Z}$ liegt. Aus $a^2 - db^2 \in \mathcal{Z}$ folgt dann $db^2 \in \mathcal{Z}$, wegen d quadratfrei somit $b \in \mathcal{Z}$. Dies zeigt die *Behauptung*.

Somit ist $\Gamma_{\mathcal{Q}(\sqrt{d})}(\mathcal{Z}) = \mathcal{Z}[\sqrt{d}]$, mit $\mathcal{Z}$-linearer Basis $(1, \sqrt{d})$.

Der Fall $p = 2$ sieht interessanter aus.

Aufgabe 5

Ad (1). Zu zeigen ist $T \overset{!}{\subseteq} \Gamma_T(R)$. Nach Voraussetzung ist $S \subseteq \Gamma_S(R)$ und $T \subseteq \Gamma_T(S)$. Es folgt

$$T \;\subseteq\; \Gamma_T(S) \;\subseteq\; \Gamma_T(\Gamma_S(R)) \;\subseteq\; \Gamma_T(\Gamma_T(R)) \overset{\text{L. 6}}{=} \Gamma_T(R) \,.$$

Ad (2). Zu zeigen ist $\Gamma_T(B) \overset{!}{\subseteq} \Gamma_T(A)$. In der Tat wird

$$\Gamma_T(B) \;=\; \Gamma_T(\Gamma_S(A)) \;\subseteq\; \Gamma_T(\Gamma_T(A)) \overset{\text{L. 6}}{=} \Gamma_T(A) \,.$$

Alternativ kann unter Verwendung von (1) wie folgt argumentiert werden. Es ist $\Gamma_T(B)$ ganz über B. Es ist B ganz über A. Dank (1) ist also $\Gamma_T(B)$ ganz über A, i.e. $\Gamma_T(B) \subseteq \Gamma_T(A)$.

Aufgabe 6

Ad (1). Sei $K := \mathrm{Quot}(R)$. Sei $x \in \Gamma_K(R)$. Wir haben zu zeigen, daß $x \overset{!}{\in} R$ liegt. Wir haben dazu nur den Fall $x \neq 0$ zu betrachten. Es genügt zu zeigen, daß $\mathrm{v}_p(x) \geqslant 0$ ist für alle Primelemente p aus $R^\times$; cf. Aufgabe 2.(6.ii). *Annahme,* es gibt ein $p \in R^\times$ prim mit $\mathrm{v}_p(x) < 0$. Da $x \in \Gamma_K(R)$, gibt es $f(X) \in R[X]$ normiert mit $f(x) = 0$. Schreibe $f(X) =: X^n + \sum_{i\in[0,n-1]} a_i X^i$, wobei $n := \deg(f)$. Es ist $x^n = -\sum_{i\in[0,n-1]} a_i x^i$. Mit Aufgabe 2.(5) wird

$$\begin{aligned} n\,\mathrm{v}_p(x) &= \mathrm{v}_p(x^n) \\ &= \mathrm{v}_p\big(-\textstyle\sum_{i\in[0,n-1]} a_i x^i\big) \\ &\geqslant \min\{\,\mathrm{v}_p(a_i x^i) \,:\, i \in [0, n-1]\,\} \\ &\geqslant \min\{\,i\,\mathrm{v}_p(x) \,:\, i \in [0, n-1]\,\} \\ &= (n-1)\,\mathrm{v}_p(x) \,, \end{aligned}$$

also $\mathrm{v}_p(x) \geqslant 0$, und wir haben einen *Widerspruch*.

Ad (2, 3). Sei R ein Integritätsbereich. *Behauptung.* Finden wir eine Abbildung $e : R^\times \to \mathbf{Z}_{\geqslant 0}$ so, daß für alle $a, b \in R^\times$ Elemente $r, s \in R$ mit $b = sa + r$ und $((r \neq 0$ und $e(r) < e(a))$ oder $r = 0)$ existieren, dann ist R ein Hauptidealbereich.

Sei dazu ein Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{a} \neq (0)$ gegeben. Wir müssen zeigen, daß $\mathfrak{a} \stackrel{!}{=} (y)$ für ein $y \in \mathfrak{a}$ ist. Wähle dazu $y \in \mathfrak{a}$ mit $y \neq 0$ und $e(y)$ minimal. Sei $x \in \mathfrak{a}^\times$. Wir haben $x \stackrel{!}{\in} (y)$ zu zeigen. Schreibe $x = sy + r$ mit $r, s \in R$ und mit $(r \neq 0$ und $e(r) < e(y))$ oder $r = 0$. Es ist $r = x - sy \in \mathfrak{a}$. Wegen der Minimalität von $e(y)$ folgt $r = 0$ und so $x = sy \in (y)$. Dies zeigt die *Behauptung.*

Sei nun $\mathbf{Z}[\mathrm{i}]^\times \to \mathbf{Z}_{\geqslant 0}$, $x \mapsto |x|^2$ (Betrag in $\mathbf{C}$ gebildet). Beachte $|a + b\mathrm{i}|^2 = a^2 + b^2$ für $a, b \in \mathbf{Z}$.

Seien $x, y \in \mathbf{Z}[\mathrm{i}]$ gegeben. Wir müssen $r, s \in \mathbf{Z}[\mathrm{i}]$ so finden, daß $x = sy + r$, i.e. $z := \frac{x}{y} = s + \frac{r}{y}$ ist, mit $|\frac{r}{y}|^2 < 1$. In der Tat hat z in $\mathbf{C}$ einen Abstand $\leqslant \frac{1}{2}\sqrt{2} < 1$ vom nächstgelegenen Punkt s in $\mathbf{Z}[\mathrm{i}] = \{\, a + b\mathrm{i} \,:\, a, b \in \mathbf{Z} \,\}$ (Abstand vom Mittelpunkt eines Quadrats mit Seitenlänge 1 zu seinen Ecken).

Sei ferner $\mathbf{Z}[\zeta_3]^\times \to \mathbf{Z}_{\geqslant 0}$, $x \mapsto |x|^2$ (Betrag in $\mathbf{C}$ gebildet). Beachte $|a + b\zeta_3|^2 = (a + b\zeta_3)(a + b\zeta_3^2) = a^2 - ab + b^2$ für $a, b \in \mathbf{Z}$.

Seien $x, y \in \mathbf{Z}[\zeta_3]$ gegeben. Wir müssen $r, s \in \mathbf{Z}[\zeta_3]$ so finden, daß $x = sy + r$, i.e. $z := \frac{x}{y} = s + \frac{r}{y}$ ist, mit $|\frac{r}{y}| < 1$ oder $r = 0$. In der Tat hat z in $\mathbf{C}$ einen Abstand $\leqslant \frac{1}{3}\sqrt{3} < 1$ vom nächstgelegenen Punkt s in $\mathbf{Z}[\zeta_3] = \{\, a + b\zeta_3 \,:\, a, b \in \mathbf{Z} \,\}$ (Abstand vom Mittelpunkt eines gleichseitigen Dreiecks mit Seitenlänge 1 zu seinen Ecken).

Ad (4). Es ist $\mathbf{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbf{Q}}(\sqrt{-5})$ nach Aufgabe 3 und also ganzabgeschlossen nach Bemerkung 8.(2).

Wir bemerken, daß $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$ ist für $a, b \in \mathbf{Q}$, und daß deswegen 2 und 3 nicht Norm eines Elementes in $\mathbf{Z}[\sqrt{-5}]$ sein können.

Wir *behaupten*, daß $\mathbf{Z}[\sqrt{-5}]$ kein Hauptidealbereich ist. Wir zeigen dazu, daß $(2, 1+\sqrt{-5})$ kein Hauptideal ist. *Annahme,* doch. Dann gibt es ein $x \in \mathbf{Z}[\sqrt{-5}]$ mit $(2, 1 + \sqrt{-5}) = (x)$. Somit gibt es $y, z \in \mathbf{Z}[\sqrt{-5}]$ mit $xy = 2$ und $xz = 1 + \sqrt{-5}$. Es folgt

$$\begin{array}{rcccl} \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x) \cdot \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(y) & = & \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(2) & = & 4 \\ \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x) \cdot \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(z) & = & \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(1 + \sqrt{-5}) & = & 6 \end{array}$$

Folglich ist $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x)$ ein Teiler von 2. Mit der obigen Bemerkung folgt $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x) = 1$. Also ist $(2, 1 + \sqrt{-5}) = (x) = \mathbf{Z}[\sqrt{-5}]$; cf. Lemma 20.(4). Betrachte den Ringmorphismus

$$\begin{array}{rcl} \mathbf{Z}[X]/(X^2 + 5) & \xrightarrow{\varphi} & \mathbf{F}_2 \\ X & \longmapsto & 1\,; \end{array}$$

wohldefiniert dank $1^2 + 5 = 0$ in $\mathbf{F}_2$; cf. **[5,** §1.4.3, §1.6]. Isomorphe Ersetzung entlang dem Ringisomorphismus $\mathbf{Z}[X]/(X^2 + 5) \xrightarrow{\sim} \mathbf{Z}[\sqrt{-5}]$, $X \mapsto \sqrt{-5}$ gibt den Ringmorphismus

$$\begin{array}{rcl} \mathbf{Z}[\sqrt{-5}] & \xrightarrow{\psi} & \mathbf{F}_2 \\ \sqrt{-5} & \longmapsto & 1\,. \end{array}$$

Es ist ψ surjektiv. Es ist $\psi((2, 1 + \sqrt{-5})) = (\psi(2), \psi(1 + \sqrt{-5})) = (0) \neq \mathbf{F}_2 = \psi(\mathbf{Z}[\sqrt{-5}])$. Dieser *Widerspruch* zeigt die Behauptung.

Alternativ kann man auch zeigen, daß $2 \in \mathbf{Z}[\sqrt{-5}]$ irreduzibel, aber nicht prim ist. Es ist nicht prim, da

$$\mathbf{Z}[\sqrt{-5}]/(2) \;\simeq\; (\mathbf{Z}[X]/(X^2 + 5))/(2) \;=\; \mathbf{Z}[X]/(X^2 + 5,\, 2) \;\simeq\; \mathbf{F}_2[X]/(X^2 + 5) \;=\; \mathbf{F}_2[X]/((X + 1)^2)$$

kein Integritätsbereich ist, da in letzterem $(X+1)+((X+1)^2)$ ungleich 0 ist, im Quadrat aber verschwindet. Es ist irreduzibel, da $2 = xy$ mit $x,\ y \in \mathbf{Z}[\sqrt{-5}]$ auf $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x) \cdot \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(y) = \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(xy) = \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(2) = 4$ führt, was wegen der Bemerkung eingangs entweder $\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(x) = 1$ und damit $x \in \mathrm{U}(\mathbf{Z}[\sqrt{-5}])$ liefert oder dito für y; cf. Lemma 20.(4). Daher kann $\mathbf{Z}[\sqrt{-5}]$ nach Aufgabe 2.(2) kein Hauptidealbereich sein.

Aufgabe 7

Schreibe $\delta := \sqrt[3]{2}$ und $\zeta := \zeta_3$.

Ad (1). Es ist $(X^3 - 2) = (X - \delta)(X - \zeta\delta)(X - \zeta^2\delta)$. Folglich ist $\mathbf{Q}(\delta, \zeta\delta, \zeta^2\delta)$ ein Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbf{Q}[X]$ und damit galoisch über $\mathbf{Q}$; cf. [**5,** §3.5.1.4].

Da $\zeta = (\zeta\delta) \cdot (\delta)^{-1}$, ist

$$L \ := \ \mathbf{Q}(\delta, \zeta) \ = \ \mathbf{Q}(\delta, \zeta\delta, \zeta^2\delta) \ .$$

Es ist $\mu_{\delta,\mathbf{Q}}(X) = X^3 - 2$. Denn um $X^3 - 2 \in \mathbf{Q}[X]$ als irreduzibel nachzuweisen, genügt es, es in $\mathbf{Z}[X]$ als irreduzibel nachzuweisen; cf. Aufgabe 2.(7). Nun ist es aber bereits in $\mathbf{F}_7[X]$ mangels Nullstelle irreduzibel.

Alternativ kann man das Eisensteinkriterium heranziehen.

Es ist $\zeta \notin \mathbf{Q}(\delta) \subseteq \mathbf{R}$. Also bleibt $\mu_{\zeta,\mathbf{Q}}(X) = X^2 + X + 1$ mangels Nullstelle irreduzibel in $\mathbf{Q}(\delta)[X]$. Somit ist

$$[L : \mathbf{Q}] \ = \ [\mathbf{Q}(\delta, \zeta) : \mathbf{Q}] \ = \ [\mathbf{Q}(\delta, \zeta) : \mathbf{Q}(\delta)] \cdot [\mathbf{Q}(\delta) : \mathbf{Q}] \ = \ 2 \cdot 3 \ = \ 6 \ .$$

Nun weiß man zwar aus Gradgründen, daß $\mathrm{Gal}(L|\mathbf{Q}) \simeq \mathrm{S}_3$ ist, denn $[L : \mathbf{Q}] = (\deg(X^3 - 2))!$; cf. [**5,** §3.4.1]. Wir müssen die Elemente von $\mathrm{Gal}(L|\mathbf{Q})$ aber kennen.

Es ist $\mathrm{Gal}(\mathbf{Q}(\zeta)|\mathbf{Q}) = \{ \mathrm{id}_{\mathbf{Q}(\zeta)}, \sigma \}$, wobei $\sigma : \mathbf{Q}(\zeta) \xrightarrow{\sim} \mathbf{Q}(\zeta)$, $\zeta \mapsto \bar{\zeta} = \zeta^2$.

Da $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 2$, ist $[L : \mathbf{Q}(\zeta)] = 3$ und also $\mu_{\delta,\mathbf{Q}(\zeta)}(X) = X^3 - 2$; ein echter Teiler von $X^3 - 2$ wäre unmöglich.

Für jedes Element der Menge der Nullstellen

$$\{ \underbrace{\delta}_{=:\, z_1}, \underbrace{\zeta\delta}_{=:\, z_2}, \underbrace{\zeta^2\delta}_{=:\, z_3} \}$$

von $X^3 - 2$ in L erhalten wir eine Fortsetzung von $\mathrm{id}_{\mathbf{Q}(\zeta)}$ resp. von σ zu einem Automorphismus von L, indem δ auf eine dieser Nullstellen geschickt wird; cf. [**5,** 2.3.4].

Wir erhalten so folgende Liste von Elementen von $\mathrm{Gal}(L|\mathbf{Q})$.

$$\begin{array}{lcl}
L & \xrightarrow{\sim} & L \\
\\
\zeta & \overset{\tau_1}{\longmapsto} & \zeta \\
\delta & \overset{\tau_1}{\longmapsto} & \delta \\
\\
\zeta & \overset{\tau_2}{\longmapsto} & \zeta \\
\delta & \overset{\tau_2}{\longmapsto} & \zeta\delta \\
\\
\zeta & \overset{\tau_3}{\longmapsto} & \zeta \\
\delta & \overset{\tau_3}{\longmapsto} & \zeta^2\delta \\
\\
\zeta & \overset{\tau_4}{\longmapsto} & \zeta^2 \\
\delta & \overset{\tau_4}{\longmapsto} & \delta \\
\\
\zeta & \overset{\tau_5}{\longmapsto} & \zeta^2 \\
\delta & \overset{\tau_5}{\longmapsto} & \zeta\delta \\
\\
\zeta & \overset{\tau_6}{\longmapsto} & \zeta^2 \\
\delta & \overset{\tau_6}{\longmapsto} & \zeta^2\delta
\end{array}$$

Es ist dabei $\tau_1 = \mathrm{id}_L$.

Auf der Menge der Nullstellen operieren diese Elemente wie folgt, wenn wir nur die Indizes notieren und mit den enstandenen Permutationen identifizieren.

$$\begin{array}{lcl}
\tau_1 & = & \mathrm{id} \\
\tau_2 & = & (1,2,3) \\
\tau_3 & = & (1,3,2) \\
\tau_4 & = & (2,3) \\
\tau_5 & = & (1,2) \\
\tau_6 & = & (1,3)
\end{array}$$

Zwischenkörper sind die folgenden.

$$\begin{array}{lcl}
\mathrm{Fix}_1(L) & = & L \\
\mathrm{Fix}_{\langle(1,2,3)\rangle}(L) & = & \mathbf{Q}(\zeta) \\
\mathrm{Fix}_{\langle(1,2)\rangle}(L) & = & \mathbf{Q}(\zeta^2\delta) \\
\mathrm{Fix}_{\langle(1,3)\rangle}(L) & = & \mathbf{Q}(\zeta\delta) \\
\mathrm{Fix}_{\langle(2,3)\rangle}(L) & = & \mathbf{Q}(\delta) \\
\mathrm{Fix}_{\mathrm{S}_3}(L) & = & \mathbf{Q}
\end{array}$$

Ad (2). Dank (1) ist $L|\mathbf{Q}$ galoisch.

Es ist $\tau_3(\mathbf{Q}(\delta)) = \mathbf{Q}(\zeta^2\delta)$. Ein Teilkörper, der sowohl $\mathbf{Q}(\delta)$ als auch $\mathbf{Q}(\zeta^2\delta)$ enthält, ist bereits gleich L.

Also ist $\mathbf{Q}(\delta,\zeta)$ Zerfällungskörper von $\mathbf{Q}(\delta)|\mathbf{Q}$; cf. Definition 9.

Ad (3). Es ist $\mathbf{Q}(\zeta)|\mathbf{Q}$ galoisch, e.g. da $\mathbf{Q}(\zeta) = \mathrm{Fix}_{\langle(1,2,3)\rangle}(L)$ ist und da $\langle(1,2,3)\rangle$ ein Normalteiler in S_3 ist. Also ist $\mathbf{Q}(\zeta)$ Zerfällungskörper von $\mathbf{Q}(\zeta)|\mathbf{Q}$. Wegen $L \neq \mathbf{Q}(\zeta)$ kann L kein Zerfällungskörper von $\mathbf{Q}(\zeta)|\mathbf{Q}$ sein; cf. Lemma 11.(2).

Wir erkennen auch direkt, daß $\tau_i(\mathbf{Q}(\zeta)) = \mathbf{Q}(\zeta)$ ist für $i \in [1,6]$. Also ist der kleinste Teilkörper, der all diese Bildkörper enthält, gleich $\mathbf{Q}(\zeta)$ und damit nicht gleich L. Auch dies zeigt, daß L kein Zerfällungskörper von $\mathbf{Q}(\zeta)|\mathbf{Q}$ ist.

Ad (4).

Direkt. Bezüglich der Basis $(1, \delta, \delta^2)$ von $\mathbf{Q}(\delta)$ hat λ_δ die beschreibende Matrix $\left(\begin{smallmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Also ist

$$\mathrm{Tr}_{\mathbf{Q}(\delta)|\mathbf{Q}}(\delta) \;=\; \mathrm{tr}\left(\begin{smallmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right) \;=\; 0\,, \qquad \mathrm{N}_{\mathbf{Q}(\delta)|\mathbf{Q}}(\delta) \;=\; \det\left(\begin{smallmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right) \;=\; 2\,.$$

Nach Lemma 15. Es ist $\mathrm{Gal}(L|\mathbf{Q}(\delta)) = \langle (2,3) \rangle$. Es ist

$$\mathrm{S}_3 \;=\; \mathrm{id}\langle (2,3)\rangle \sqcup (1,2,3)\langle (2,3)\rangle \sqcup (1,3,2)\langle (2,3)\rangle \;=\; \tau_1\langle (2,3)\rangle \sqcup \tau_2\langle (2,3)\rangle \sqcup \tau_3\langle (2,3)\rangle$$

Also wird

$$\mathrm{Tr}_{\mathbf{Q}(\delta)|\mathbf{Q}}(\delta) \;=\; \tau_1(\delta) + \tau_2(\delta) + \tau_3(\delta) = \delta + \zeta\delta + \zeta^2\delta \;=\; 0$$

und

$$\mathrm{N}_{\mathbf{Q}(\delta)|\mathbf{Q}}(\delta) \;=\; \tau_1(\delta) \cdot \tau_2(\delta) \cdot \tau_3(\delta) = \delta \cdot \zeta\delta \cdot \zeta^2\delta \;=\; 2\,.$$

Aufgabe 8

Wir brauchen nur den Fall $\mathrm{char}\, K = p > 0$ betrachten.

Wir müssen zeigen, daß die Abbildung $\mathrm{Frob}_L : L \twoheadrightarrow L$, $x \mapsto x^p$ surjektiv ist.

Zum einen ist L ein K-Vektorraum vermöge der Multiplikation $x \cdot_1 y := xy$ für $x \in K$ und $y \in L$, genannt L_1.

Zum anderen ist L ein K-Vektorraum vermöge der Multiplikation $x \cdot_2 y := x^p y$ für $x \in K$ und $y \in L$, genannt L_2.

Es ist $\mathrm{Frob}_L(x \cdot_1 y) = \mathrm{Frob}_L(xy) = (xy)^p = x^p y^p = x \cdot_2 \mathrm{Frob}_L(y)$. Also ist Frob_L eine K-lineare Abbildung von L_1 nach L_2. Um die Bijektivität von Frob_L zu zeigen, genügt es, $\dim_K L_1 \stackrel{!}{=} \dim_K L_2$ nachzuweisen.

Sei $(y_1, \ldots, y_n)$ eine K-lineare Basis von L_1. Wir *behaupten,* daß $(y_1, \ldots, y_n)$ auch eine K-lineare Basis von L_2 ist.

Zur linearen Unabhängigkeit. Ist $\sum_{i\in[1,n]} x_i \cdot_2 y_i = 0$, wobei $x_i \in K$ für $i \in [1,n]$, dann ist $\sum_{i\in[1,n]} x_i^p \cdot_1 y_i = 0$, also $x_i^p = 0$ und somit $x_i = 0$ für $i \in [1,n]$.

Zum Erzeugendensystem. Sei $z \in L$ gegeben. Wir schreiben $z = \sum_{i\in[1,n]} x_i \cdot_1 y_i$ mit $x_i \in K$ für $i \in [1,n]$. Da K perfekt ist, gibt es $x_i' \in K$ mit $x_i'^p = x_i$ für $i \in [1,n]$. Dann wird $\sum_{i\in[1,n]} x_i' \cdot_2 y_i = \sum_{i\in[1,n]} x_i'^p \cdot_1 y_i = \sum_{i\in[1,n]} x_i \cdot_1 y_i = z$.

Aufgabe 9

Ad (1). Es zerfällt G in eine disjunkte Vereinigung von 4 Linksnebenklassen modulo U. Aus jeder der 4 Nebenklassen, bestehend aus je 6 Elementen, darf ein beliebiger Repräsentant gewählt werden. Folglich gibt es 6^4 Teilmengen T mit $G = \bigsqcup_{\sigma\in T} \sigma U$.

Ad (2). Wir haben die folgenden Nebenklassen.

$$\begin{aligned} U &= \{\mathrm{id}, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\} \\ (1,4)U &= \{(1,4), (1,2,4), (1,4)(2,3), (1,3,4), (1,2,3,4), (1,3,2,4)\} \\ (2,4)U &= \{(2,4), (1,4,2), (2,3,4), (1,3)(2,4), (1,4,2,3), (1,3,4,2)\} \\ (3,4)U &= \{(3,4), (1,2)(3,4), (2,4,3), (1,4,3), (1,2,4,3), (1,4,3,2)\} \end{aligned}$$

Somit ist $T_1 := \{\mathrm{id}, (1,4)(2,3), (1,3)(2,4), (1,2)(3,4)\}$ ein Repräsentantensystem wie in (1) verlangt, für welches zugleich $T_1 \leqslant G$ gilt.

Ferner ist $T_2 := \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$ ein Repräsentantensystem wie in (1) verlangt, für welches zugleich $T_2 \leqslant G$ gilt.

Schließlich ist $T_1 \simeq \mathrm{C}_2 \times \mathrm{C}_2 \not\simeq \mathrm{C}_4 \simeq T_2$.

Aufgabe 10

Ad (1). Da S unter Multiplikation abgeschlossen ist und $1 \in S$ liegt, zeigt Bruchrechnung, daß $S^{-1}A \subseteq K$ ein Teilring ist : es ist die 1 in $S^{-1}A$ enthalten; die Differenz und das Produkt zweier Elemente in $S^{-1}A$ ist wieder in $S^{-1}A$.

> Daß die p-ganzen Elemente aus Aufgabe 2.(6) einen Teilring des Quotientenkörpers bilden, ist hiervon der Spezialfall, bei dem S aus der Teilmenge der Elemente besteht, die bei p die Bewertung 0 haben.

Da $1 \in S$, ist A Teilring von $S^{-1}A$.

Zeigen wir, daß es für jeden kommutativen Ring B und jeden Ringmorphismus $\varphi : A \to B$ mit $\varphi(S) \subseteq \mathrm{U}(B)$ genau einen Ringmorphismus $\psi : S^{-1}A \to B$ mit $\psi|_A = \varphi$ gibt.

Eindeutigkeit. Ist $\psi|_A = \varphi$, so ist $\psi(\frac{a}{1}) = \varphi(a)$ für $a \in A$. Ist $s \in S$, so folgt hieraus $\psi(\frac{1}{s}) = \psi((\frac{s}{1})^{-1}) = \psi(\frac{s}{1})^{-1} = \varphi(a)^{-1}$. Zusammen muß also $\psi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$ sein.

Existenz. Setze $\psi(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$ für $a \in A$ und $s \in S$.

Das ist wohldefiniert, da zum einen $\varphi(s) \in \mathrm{U}(B)$ für alle $s \in S$ ist und da zum anderen für $t \in S$ sich $\varphi(ta)\varphi(ts)^{-1} = \varphi(t)\varphi(a)\varphi(s)^{-1}\varphi(t)^{-1} = \varphi(a)\varphi(s)^{-1}$ ergibt.

Es ist $\psi(\frac{1}{1}) = \varphi(1)\varphi(1)^{-1} = 1$.

Es ist ψ mit der Multiplikation verträglich, da

$$\psi(\frac{a}{s}\frac{a'}{s'}) \;=\; \psi(\frac{aa'}{ss'}) \;=\; \varphi(aa')\varphi(ss')^{-1} \;=\; \varphi(a)\varphi(s)^{-1}\varphi(a')\varphi(s')^{-1} \;=\; \psi(\frac{a}{s})\psi(\frac{a'}{s'})$$

ist für a, $a' \in A$ und s, $s' \in S$.

Um zu zeigen, daß ψ mit der Addition verträglich ist, dürfen wir wegen Wohldefiniertheit annehmen, daß die Summanden denselben Nenner aufweisen. Es wird

$$\psi(\frac{a}{s} + \frac{a'}{s}) \;=\; \psi(\frac{a+a'}{s}) \;=\; \varphi(a+a')\varphi(s)^{-1} \;=\; \varphi(a)\varphi(s)^{-1} + \varphi(a')\varphi(s)^{-1} \;=\; \psi(\frac{a}{s}) + \psi(\frac{a'}{s})$$

für a, $a' \in A$ und $s \in S$.

Zeigen wir nun, daß $S^{-1}\mathfrak{a}$ ein Ideal in $S^{-1}A$ ist. Sind $\frac{a}{s}$ und $\frac{a'}{s'}$ in $S^{-1}\mathfrak{a}$ gegeben mit a, $a' \in \mathfrak{a}$ und s, $s' \in S$ und $\frac{b}{t}$ und $\frac{b'}{t'}$ in $S^{-1}A$ gegeben mit b, $b' \in A$ und t, $t' \in S$, dann ist

$$\frac{b}{t}\frac{a}{s} + \frac{b'}{t'}\frac{a'}{s'} \;=\; \frac{bat's' + tsb'a'}{tst's'} \;\in\; S^{-1}\mathfrak{a}\,.$$

Zudem ist $0 \in S^{-1}A$. Also ist $S^{-1}\mathfrak{a} \subseteq S^{-1}A$ ein Ideal.

Wir vereinbaren noch, daß ein Bruch $\frac{a}{s} \in S^{-1}A$ mit $a \in A$ und $s \in S$ geschrieben werde, wenn nichts anderes gesagt wird.

Sei $\mathfrak{p} \in \mathrm{Ideale}^{A\smallsetminus S}_{\mathrm{prim}}(A)$.

1. Wir *behaupten*, daß für $\frac{a}{s} \in S^{-1}A$ genau dann $\frac{a}{s} \in S^{-1}\mathfrak{p}$ liegt, wenn $a \in \mathfrak{p}$ liegt. Liegt $a \in \mathfrak{p}$, dann ist $\frac{a}{s} \in S^{-1}\mathfrak{p}$. Liegt umgekehrt $\frac{a}{s} \in S^{-1}\mathfrak{p}$, dann gibt es $\frac{x}{t}$ mit $x \in \mathfrak{p}$ und $t \in S$ derart, daß $\frac{a}{s} = \frac{x}{t}$ ist. Dann aber ist auch $at = xs \in \mathfrak{p}$. Da $t \notin \mathfrak{p}$, folgt $a \in \mathfrak{p}$.

2. Wir *behaupten,* es ist $S^{-1}\mathfrak{p} \overset{!}{\in} \mathrm{Ideale}_{\mathrm{prim}}(S^{-1}A)$. Seien $\frac{a}{s}$ und $\frac{a'}{s'}$ in $S^{-1}A$ gegeben mit $\frac{a}{s} \cdot \frac{a'}{s'} \in S^{-1}\mathfrak{p}$. Gemäß 1. folgt $aa' \in \mathfrak{p}$, also o.E. $a \in \mathfrak{p}$ und somit $\frac{a}{s} \in S^{-1}\mathfrak{p}$. Dies zeigt die *Behauptung.*

3. Wir *behaupten,* es ist $\mathfrak{p} \overset{!}{=} (S^{-1}\mathfrak{p}) \cap A$. Zunächst ist $\mathfrak{p} \subseteq (S^{-1}\mathfrak{p}) \cap A$. Sei umgekehrt $a \in A$ mit $a = \frac{a}{1} \in S^{-1}\mathfrak{p}$ gegeben. Dann ist gemäß 1. auch $a \in \mathfrak{p}$. Dies zeigt die *Behauptung.*

Sei $\mathfrak{q} \in \mathrm{Ideale}_{\mathrm{prim}}(S^{-1}A)$ gegeben.

4. Wir *behaupten* $\mathfrak{q} \cap A \overset{!}{\in} \mathrm{Ideale}^{A \smallsetminus S}_{\mathrm{prim}}(A)$. Es ist $\mathfrak{q} \cap A$ ein Ideal von A, da $0 \in \mathfrak{q}$ und da für $y,\ y' \in \mathfrak{q} \cap A$ und $a,\ a' \in A$ sich $ay + a'y' \in \mathfrak{q} \cap A$ ergibt. Es ist $\mathfrak{q} \cap A$ ein Primideal von A, da für $a,\ a' \in A$ mit $aa' \in \mathfrak{q} \cap A$ sich o.E. $a \in \mathfrak{q}$ und also $a \in \mathfrak{q} \cap A$ ergibt. Es ist $(A \cap \mathfrak{q}) \cap S = \emptyset$, da ansonsten $s \in (A \cap \mathfrak{q}) \cap S$ läge, und also auch $1 = \frac{1}{s} \cdot s \in \mathfrak{q}$ wäre, was wegen $\mathfrak{q} \subseteq S^{-1}A$ prim nicht der Fall ist. Dies zeigt die *Behauptung.*

Also haben wir die Bijektion

$$\begin{array}{rcl} \mathrm{Ideale}^{A \smallsetminus S}_{\mathrm{prim}}(A) & \xrightarrow{\sim} & \mathrm{Ideale}_{\mathrm{prim}}(S^{-1}A) \\ \mathfrak{p} & \longmapsto & S^{-1}\mathfrak{p} \\ \mathfrak{q} \cap A & \longmapsfrom & \mathfrak{q} \end{array}$$

Ad (2). Die behauptete Bijektion ist ein Spezialfall der Bijektion aus (1).

Da diese die Teilmengenrelation respektiert, da $\mathfrak{p} = A \smallsetminus (A \smallsetminus \mathfrak{p})$ und da $\mathrm{Ideale}^{\mathfrak{p}}_{\mathrm{prim}}(A)$ das terminale Element $\mathfrak{p}$ enthält, enthält auch $\mathrm{Ideale}_{\mathrm{prim}}(A_{\mathfrak{p}})$ das terminale Element $\mathfrak{p}_{\mathfrak{p}}$.

Wir *behaupten* die Existenz des folgenden Körperisomorphismus.

$$\begin{array}{rcl} \mathrm{Quot}(A/\mathfrak{p}) & \xrightarrow{\sim} & A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} \\ \frac{a+\mathfrak{p}}{s+\mathfrak{p}} & \longmapsto & \frac{a}{s} + \mathfrak{p}_{\mathfrak{p}} \\ \frac{a+\mathfrak{p}}{s+\mathfrak{p}} & \longmapsfrom & \frac{a}{s} + \mathfrak{p}_{\mathfrak{p}} \end{array}$$

Wir zeigen, daß $\to$ ein wohldefinierter Ringmorphismus ist. Ausgehend vom komponierten Ringmorphismus $A \to A_{\mathfrak{p}} \to A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$, $a \mapsto \frac{a}{1} \mapsto \frac{a}{1} + \mathfrak{p}_{\mathfrak{p}}$, welcher $\mathfrak{p}$ auf 0 schickt, erhalten wir zunächst den induzierten Ringmorphismus $A/\mathfrak{p} \to A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$, $a + \mathfrak{p} \mapsto \frac{a}{1} + \mathfrak{p}_{\mathfrak{p}}$. Da nun alle Elemente aus $(A/\mathfrak{p})^\times$, also alle von der Form $s + \mathfrak{p}$ mit $s \in A \smallsetminus \mathfrak{p}$, unter diesem Morphismus nach $\mathrm{U}(A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}})$ abgebildet werden, erhalten wir mit der universellen Eigenschaft aus (1), angewandt auf $S := (A/\mathfrak{p})^\times$ und $S^{-1}(A/\mathfrak{p}) = \mathrm{Quot}(A/\mathfrak{p})$ den induzierten Morphismus

$$\begin{array}{rcl} \mathrm{Quot}(A/\mathfrak{p}) & \longrightarrow & A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} \\ \frac{a+\mathfrak{p}}{s+\mathfrak{p}} & \longmapsto & (\frac{a}{1} + \mathfrak{p}_{\mathfrak{p}})(\frac{s}{1} + \mathfrak{p}_{\mathfrak{p}})^{-1} \ = \ \frac{a}{s} + \mathfrak{p}_{\mathfrak{p}} \ . \end{array}$$

Wir zeigen, daß $\leftarrow\!\shortmid$ ein wohldefinierter Ringmorphismus ist. Ausgehend vom komponierten Ringmorphismus $A \to A/\mathfrak{p} \to \mathrm{Quot}(A/\mathfrak{p})$, $a \mapsto a + \mathfrak{p} \mapsto \frac{a+\mathfrak{p}}{1+\mathfrak{p}}$, welcher $A \smallsetminus \mathfrak{p}$ nach $\mathrm{U}(\mathrm{Quot}(A/\mathfrak{p})) = (A/\mathfrak{p})^\times$ schickt, erhalten wir zunächst dank der universellen Eigenschaft aus (1) den induzierten Ringmorphismus $A_{\mathfrak{p}} \to \mathrm{Quot}(A/\mathfrak{p})$, $\frac{a}{s} \mapsto (\frac{a+\mathfrak{p}}{1+\mathfrak{p}})(\frac{s+\mathfrak{p}}{1+\mathfrak{p}})^{-1} = \frac{a+\mathfrak{p}}{s+\mathfrak{p}}$. Dieser schickt $\mathfrak{p}_{\mathfrak{p}}$ auf 0, liefert also den Morphismus

$$\begin{array}{rcl} \mathrm{Quot}(A/\mathfrak{p}) & \longleftarrow & A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} \\ \frac{a+\mathfrak{p}}{s+\mathfrak{p}} & \longmapsfrom & \frac{a}{s} + \mathfrak{p}_{\mathfrak{p}} \ . \end{array}$$

Die Morphismen $\mapsto$ und $\leftarrow\!\shortmid$ kehren sich gegenseitig um. Also liegt in beiden Richtungen ein Isomorphismus vor.

Ist schließlich $\mathfrak{p} \subseteq A$ maximal, dann $A/\mathfrak{p}$ ein Körper, also $A/\mathfrak{p} = \mathrm{Quot}(A/\mathfrak{p})$, und der eben gezeigte Isomorphismus läuft von $A/\mathfrak{p}$ nach $A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$.

Aufgabe 11

Ad (1).

Wir wenden Aufgabe 10.(1) an mit $S = A^\times$ und also $S^{-1}A = \mathrm{Quot}(A)$. Da φ als Körpermorphismus injektiv ist, ist in der Tat $\varphi(S) = \varphi(A^\times) \subseteq L^\times = \mathrm{U}(L)$; cf. [**5,** Aufgabe 7.(1)]. Also gibt es einen eindeutigen Körpermorphismus $\psi : \mathrm{Quot}(A) \to L$ mit $\psi|_A = \varphi$.

> Beachte, daß ψ wie jeder Körpermorphismus injektiv ist. In der Praxis identifiziert man daher oft $\mathrm{Quot}(A)$ und $\psi(\mathrm{Quot}(A)) \subseteq L$ entlang ψ.

Ad (2). Wenden wir (1) an auf die Einbettung $B \xrightarrow{\varphi} \mathrm{Quot}(A)$, so erhalten wir den Morphismus $\psi : \mathrm{Quot}(B) \to \mathrm{Quot}(A)$, $\frac{x}{y} \mapsto \varphi(x)\varphi(y)^{-1}$, letzteres zu bilden in $\mathrm{Quot}(A)$.

Wie jeder Körpermorphismus ist ψ injektiv.

Wir *behaupten*, daß ψ surjektiv ist. Seien $v \in A$ und $u \in A^\times$ gegeben. Wir haben zu zeigen, daß $\frac{v}{u}$ im Bild von ψ liegt.

Es sind $u, v \in B$. Es wird

$$\psi(\frac{v}{u}) \;=\; \varphi(v)\varphi(u)^{-1} \;=\; v \cdot u^{-1} \;=\; \frac{v}{1} \cdot \frac{1}{u} \;=\; \frac{v}{u}\,.$$

Dies zeigt die *Behauptung*. Damit ist ψ ein Isomorphismus.

Es bleibt zu zeigen, daß $\psi^{-1} : \mathrm{Quot}(A) \to \mathrm{Quot}(B)$ in der Tat $\frac{v}{u}$ auf $\frac{v}{u}$ abbildet für $v \in A$ und $u \in A^\times$. Aber dies folgt aus $\psi(\frac{v}{u}) = \frac{v}{u}$, wie eben verifiziert.

> Auch hier identifiziert man oft $\mathrm{Quot}(A) = \mathrm{Quot}(B)$ entlang ψ.

Aufgabe 12

Die Aussage ist falsch.

Sei $K := \mathbf{Q}$. Sei $A := \mathbf{Z}$. Sei $L := \mathbf{Q}(\mathrm{i})$. Es ist $B = \Gamma_L(A) = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Sei $y := \frac{1}{5}(3 + 4\mathrm{i})$. Es ist $\mathrm{N}_{L|K}(y) = \frac{1}{5}(3 + 4\mathrm{i}) \cdot \frac{1}{5}(3 - 4\mathrm{i}) = 1 \in \mathrm{U}(A)$.

Aber es ist $y \notin \mathbf{Z}[\mathrm{i}]$, insbesondere also nicht in $\mathrm{U}(\mathbf{Z}[\mathrm{i}])$.

> Cf. auch Lemma 20.(4).

Aufgabe 13

Ad (1). *Behauptung.* Jedes Ideal $\mathfrak{a} \subset R$ liegt in einem maximalen solchen, i.e. in einem maximalen Ideal. Sei dazu $\mathrm{Ideale}(R) \smallsetminus \{(1)\}$ die Menge der echten Ideale von R. Eine Kette T darin hat $\bigcup T$ als obere Schranke in $\mathrm{Ideale}(R) \smallsetminus \{(1)\}$, da eine A-Linearkombination zweier Elemente von $\bigcup T$ bereits in einem Element $\mathfrak{t}$ von T zu bilden ist. Also liegt gemäß Lemma von Zorn jedes Element von $\mathrm{Ideale}(R) \smallsetminus \{(1)\}$ in einem maximalen; cf. e.g. [**8,** §A.1]. Dies zeigt die *Behauptung.*

> Später werden wir sehen, daß im Falle R noethersch Bemerkung 51.(4) eingesetzt und der Gebrauch des Lemmas von Zorn vermieden werden kann. Dies trifft e.g. zu, wenn R ein Hauptidealbereich ist; cf. Bemerkung 51.(1).

Insbesondere liegt (0) in einem maximalen Ideal $\mathfrak{m}$. Wir haben einen R-linearen Isomorphismus

$$R^{\oplus k} \xrightarrow{f}_{\sim} R^{\oplus \ell} .$$

Dieser liefert einen $R/\mathfrak{m}$-linearen Isomorphismus

$$\begin{array}{rcl} (R^{\oplus k})/\mathfrak{m}(R^{\oplus k}) & \xrightarrow[\sim]{\bar{f}} & (R^{\oplus \ell})/\mathfrak{m}(R^{\oplus \ell}) \\ x + \mathfrak{m}(R^{\oplus k}) & \longmapsto & f(x) + \mathfrak{m}(R^{\oplus k}) , \end{array}$$

mit Inversem $\bar{f}^{-1} = \overline{f^{-1}}$, analog gebildet.

Ferner ist $(R^{\oplus k})/\mathfrak{m}(R^{\oplus k})$ als $R/\mathfrak{m}$-Vektorraum isomorph zu $(R/\mathfrak{m})^{\oplus k}$, hat also Dimension k. Analog hat $(R^{\oplus \ell})/\mathfrak{m}(R^{\oplus \ell})$ die Dimension ℓ als Vektorraum über $R/\mathfrak{m}$.

Dank Linearer Algebra ist also $k = \ell$.

Ad (2). Mittels isomorpher Ersetzung dürfen wir $M = R^{\oplus m}$ annehmen für ein $m \geqslant 0$. Wir führen eine Induktion über $m \geqslant 0$. Für $m = 0$ ist die Aussage richtig. Sei nun $m \geqslant 1$.

Betrachte das folgende Diagramm von R-Moduln und R-linearen Abbildungen.

$$\begin{array}{ccccc} R^{\oplus(m-1)} & \hookrightarrow & R^{\oplus m} & \xrightarrow{\pi} & R \\ \uparrow & & \uparrow & & \uparrow \\ N' & \hookrightarrow & N & \twoheadrightarrow & (r) \end{array}$$

Hierbei ist π die Projektion auf den letzten Tupeleintrag. Die horizontalen Abbildungen links sind Inklusionen von Kernen. Die vertikalen Abbildungen sind Inklusionen. Das Kompositum $N \to R$ hat als Bild einen Teilmodul von R, i.e. ein Ideal in R, welches wegen R Hauptidealbereich als (r) für ein geeignetes $r \in R$ geschrieben werden kann.

Fall $r = 0$. Es ist $N' = N$. Nach Induktion ist N' ein endlich erzeugt freier R-Modul mit $\mathrm{rk}_R(N') \leqslant \mathrm{rk}_R(R^{\oplus(m-1)}) = m - 1$. Insgesamt ist $\mathrm{rk}_R(N) \leqslant m - 1 < m = \mathrm{rk}_R(M)$.

Fall $r \neq 0$. Nach Induktion ist N' endlich erzeugt frei mit $n' := \mathrm{rk}_R(N') \leqslant m - 1$. Betrachte folgendes Diagramm von R-Moduln und R-linearen Abbildungen.

$$\begin{array}{ccccc} R^{\oplus n'} & & & & R \\ \wr \downarrow \varphi & & & \swarrow_{\psi} & \downarrow \wr \\ N' & \hookrightarrow & N & \twoheadrightarrow & (r) \end{array}$$

Die untere Zeile sei die aus vorigem Diagramm.

Der linke vertikale Isomorphismus φ sei gewählt dank N' endlich erzeugt frei.

Der rechte vertikale Isomorphismus schicke 1 auf r.

Es schicke ψ die 1 auf ein Element $n_0 \in N$, welches horizontal auf r abgebildet wird. Wir erhalten die R-lineare Abbildung

$$\begin{array}{rcl} R^{\oplus n'} \oplus R & \longrightarrow & N \\ (x, y) & \longmapsto & \varphi(x) + \psi(y) . \end{array}$$

Diese Abbildung ist, so behaupten wir, ein Isomorphismus.

Surjektivität. Sei $n \in N$ gegeben. Es wird n unter π auf yr abgebildet für ein $y \in R$. Also ist $\pi(n - yn_0) = yr - yr = 0$. Somit gibt es ein $x \in R^{\oplus n'}$ mit $\varphi(x) = n - yn_0 = n - \psi(y)$. Somit ist $n = \varphi(x) + \psi(y)$.

Injektivität. Sei $(x,y) \in R^{\oplus n'} \oplus R$ mit $\varphi(x) + \psi(y) = 0$ gegeben. Dann ist $\varphi(x) = -\psi(y) = -yn_0$. Anwendung von π liefert $0 = -yr$, also $y = 0$. Also ist $\varphi(x) = 0$ und damit auch $x = 0$.

Also ist N endlich erzeugt frei. Schließlich ist noch $\mathrm{rk}_R(N) = n' + 1 \leqslant m = \mathrm{rk}_R(M)$.

Aufgabe 14

Ad (1). Dank Elementarteilersatz gibt es invertierbare ganzzahlige Matrizen $S, T \in \mathrm{GL}_n(\mathbf{Z})$ mit $SAT = D = \mathrm{diag}(\, d_1 \,, \,\ldots\,, \, d_n \,)$; cf. [**4,** Satz 4].

Es ist $|\det(S)| = 1$ und $|\det(T)| = 1$. Also ist $|\det(A)| = |\det(D)| = d_1 \cdots d_n$.

Zunächst folgt aus $\mathbf{Z}^{n\times 1} \supseteq T\mathbf{Z}^{n\times 1}$, daß $T^{-1}\mathbf{Z}^{n\times 1} \supseteq \mathbf{Z}^{n\times 1}$ ist. Somit ist $T^{-1}\mathbf{Z}^{n\times 1} = \mathbf{Z}^{n\times 1}$. Also wird

$$\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1} \;=\; \mathbf{Z}^{n\times 1}/S^{-1}DT^{-1}\mathbf{Z}^{n\times 1} \;=\; \mathbf{Z}^{n\times 1}/S^{-1}D\mathbf{Z}^{n\times 1} \;.$$

Ferner haben wir den Isomorphismus abelscher Gruppen

$$\begin{array}{rcl} \mathbf{Z}^{n\times 1}/S^{-1}D\mathbf{Z}^{n\times 1} & \xrightarrow{\sim} & \mathbf{Z}^{n\times 1}/D\mathbf{Z}^{n\times 1} \\ x + S^{-1}D\mathbf{Z}^{n\times 1} & \longmapsto & Sx + D\mathbf{Z}^{n\times 1} \\ S^{-1}y + S^{-1}D\mathbf{Z}^{n\times 1} & \longmapsfrom & y + D\mathbf{Z}^{n\times 1} \;; \end{array}$$

wobei zu beachten ist, daß $\to$ wohldefiniert ist, da $S(S^{-1}D\mathbf{Z}^{n\times 1}) \subseteq D\mathbf{Z}^{n\times 1}$, und daß $\hookleftarrow$ wohldefiniert ist, da $S^{-1}(D\mathbf{Z}^{n\times 1}) = S^{-1}D\mathbf{Z}^{n\times 1}$.

Schließlich haben wir den Isomorphismus abelscher Gruppen

$$\begin{array}{rcl} \mathbf{Z}^{n\times 1}/D\mathbf{Z}^{n\times 1} & \xrightarrow{\sim} & \bigoplus_{i\in[1,n]} \mathbf{Z}/d_i\mathbf{Z} \\ x + D\mathbf{Z}^{n\times 1} & \longmapsto & (x_i + d_i\mathbf{Z})_i \\ x + D\mathbf{Z}^{n\times 1} & \longmapsfrom & (x_i + d_i\mathbf{Z})_i \end{array}$$

Alles in allem ist also $\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1} \simeq \bigoplus_{i\in[1,n]} \mathbf{Z}/d_i\mathbf{Z}$ als abelsche Gruppen, und somit auch

$$|\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1}| \;=\; |\bigoplus_{i\in[1,n]} \mathbf{Z}/d_i\mathbf{Z}| \;=\; |d_1 \cdots d_n| \;=\; |\det(A)| \;.$$

Ad (2). Sei $Y \xrightarrow{\iota} X$ die Inklusionsabbildung.

Wir haben den $\mathbf{Z}$-linearen Isomorphismus $\varphi_{\underline{x}} : \mathbf{Z}^{n\times 1} \xrightarrow{\sim} X$, $(a_i)_i \mapsto \sum_{i\in[1,n]} a_i x_i$ und den $\mathbf{Z}$-linearen Isomorphismus $\varphi_{\underline{y}} : \mathbf{Z}^{n\times 1} \xrightarrow{\sim} Y$, $(b_j)_j \mapsto \sum_{j\in[1,n]} b_j y_j$.

Wir haben ein kommutatives Viereck

$$\begin{array}{ccc} \mathbf{Z}^{n\times 1} & \xrightarrow{A(-)} & \mathbf{Z}^{n\times 1} \\ {\scriptstyle\varphi_{\underline{y}}}\downarrow\wr & & \wr\downarrow{\scriptstyle\varphi_{\underline{x}}} \\ Y & \xrightarrow{\;\iota\;} & X \;, \end{array}$$

denn $(b_j)_j \in \mathbf{Z}^{n\times 1}$ wird untenherum auf $\sum_{j\,\in\,[1,n]} b_j y_j \;=\; \sum_{i,\,j\,\in\,[1,n]} x_i a_{i,\,j} b_j$ geschickt, genauso wie obenherum.

Also haben wir einen induzierten $\mathbf{Z}$-linearen Isomorphismus

$$\begin{array}{rcl} \mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1} & \overset{\psi}{\xrightarrow[\sim]{}} & X/Y \\ a + A\mathbf{Z}^{n\times 1} & \longmapsto & \varphi_{\underline{x}}(a) + Y \;=\; \sum_{i\in[1,n]} a_i x_i + Y \;. \end{array}$$

Direkt verifizieren wir diesen wie folgt.

Wegen der Kommutativität des obigen Vierecks wird das Bild von $A(-)$ unter $\varphi_{\underline{x}}$ auf Y abgebildet, so daß ψ eine wohldefinierte $\mathbf{Z}$-lineare Abbildung wird.

Wegen der Kommutativität des obigen Vierecks wird Y unter $\varphi_{\underline{x}}^{-1}$ auf das Bild von $A(-)$ abgebildet, so daß auch

$$\begin{array}{ccc} \mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1} & \xleftarrow[\sim]{\tilde{\psi}} & X/Y \\ \varphi_{\underline{x}}^{-1}(x) + A\mathbf{Z}^{n\times 1} & \longmapsto & x + Y \end{array}$$

eine wohldefinierte Abbildung ist.

Nach Konstruktion ist $\psi \circ \tilde{\psi} = \mathrm{id}_{X/Y}$ und $\tilde{\psi} \circ \psi = \mathrm{id}_{\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1}}$. Folglich ist ψ ein $\mathbf{Z}$-linearer Isomorphismus.

Somit ist

$$|X/Y| \;=\; |\mathbf{Z}^{n\times 1}/A\mathbf{Z}^{n\times 1}| \;\overset{(1)}{=}\; |\det(A)|\,.$$

Ad (3). Es ist $Y \subseteq \mathcal{O}_K \overset{\text{B. 30}}{\subseteq} \mathcal{O}_K^{\#} \subseteq Y^{\#}$. Sei $\underline{y'} := (\, y_i' \,:\, i \in [1,n]\,)$ die zu $\underline{y}$ duale Basis, i.e. $\mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j') = \partial_{i,\,j}$ für $i,\, j \,\in\, [1,n]$. Dann ist $\underline{y'}$ eine $\mathbf{Z}$-lineare Basis von $Y^{\#}$; cf. Lemma 31.(3).

Schreibe $y_j = \sum_{i\in[1,n]} a_{i,\,j} y_i'$ für $j \in [1,n]$, wobei $A := (a_{i,\,j})_{i,\,j} \in \mathbf{Z}^{n\times n}$.

Wir *behaupten* $a_{i,\,j} \overset{!}{=} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j)$ für $i,\, j \,\in\, [1,n]$, i.e. $y_j \overset{!}{=} \sum_{i\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j) y_i'$ für $j \in [1,n]$. Da die Spurbilinearform nichtausgeartet ist, genügt es hierfür,

$$\mathrm{Tr}_{K|\mathbf{Q}}(y_j\, y_k) \;\overset{!}{=}\; \mathrm{Tr}_{K|\mathbf{Q}}(\sum_{i\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j) y_i'\, y_k)$$

zu zeigen für $j, k \in [1,n]$; cf. Lemma 22. In der Tat wird

$$\begin{array}{rcl} \mathrm{Tr}_{K|\mathbf{Q}}(\sum_{i\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j) y_i'\, y_k) & = & \sum_{i\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j)\, \mathrm{Tr}_{K|\mathbf{Q}}(y_i'\, y_k) \\ & = & \sum_{i\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(y_i\, y_j) \partial_{i,k} \\ & = & \mathrm{Tr}_{K|\mathbf{Q}}(y_k\, y_j) \\ & = & \mathrm{Tr}_{K|\mathbf{Q}}(y_j\, y_k)\,. \end{array}$$

Dies zeigt die *Behauptung.*

Somit wird

$$|Y^{\#}/Y| \;\overset{(2)}{=}\; |\det(A)| \;=\; |\det((\mathrm{Tr}_{K|\mathbf{Q}}(y_i y_j))_{i,\,j})| = |\det(\mathrm{Gram}_{K|\mathbf{Q},\,\underline{y}})| \;\overset{\text{L. 22}}{=}\; |\Delta_{K|\mathbf{Q},\,\underline{y}}|\,.$$

Aufgabe 15

Ad (1). Die Aussage ist falsch.

Sei $K := \mathbf{Q}$, $A := \mathbf{Z}$, $\delta := \sqrt[3]{2}$, $L := \mathbf{Q}(\delta)$ und $\underline{g} = (1, \delta, \delta^2)$ eine $\mathbf{Z}$-lineare Basis des Rings $\mathbf{Z}[\delta]$.

> Dann ist in der Tat $\mathbf{Z}[\delta] = \mathcal{O}_{\mathbf{Q}(\delta)}$, aber das werden wir erst in Aufgabe 19 ermitteln.

Schreibe $\zeta := \zeta_3$. Dann ist der Zerfällungskörper von $L|K$ gleich $E := \mathbf{Q}(\delta, \zeta)$. Es ist

$$\{\, \sigma(\delta) \,:\, \sigma \in \mathrm{Gal}(E|K)\,\} \;=\; \{\delta, \zeta\delta, \zeta^2\delta\}\,;$$

cf. Lösung zu Aufgabe 7.(1). Also ist

$$\det(\mathrm{Vand}_{L|K,\underline{g}}) \;=\; (\zeta\delta - \delta)(\zeta^2\delta - \delta)(\zeta^2\delta - \zeta\delta) \;=\; 2(\zeta - 1)(\zeta^2 - 1)(\zeta^2 - \zeta) \;=\; -6\mathrm{i}\sqrt{3} \;\notin\; \mathbf{Z}$$

Cf. Bemerkung 25 und Beispiel 26.(2).

Ad (2). Die Aussage ist richtig.

Schreibe $d := \det(\mathrm{Vand}_{L|K,\underline{g}}) \in L$; cf. Lemma 24.

Es ist $d^2 := \det(\mathrm{Vand}_{L|K,\underline{g}})^2 = \Delta_{L|K,\underline{g}} \in A \subseteq K$, cf. Lemma 36. Also ist $[K(d) : K] = \deg(\mu_{d,K}(X)) \in \{1, 2\}$. Da

$$[L : K] \;=\; [L : K(d)][K(d) : K]$$

ist und da $[L : K]$ ungerade ist, folgt $[K(d) : K] = 1$, i.e. $d \in K$.

Da die Einträge von $\mathrm{Vand}_{L|K,\underline{g}}$ gemäß Lemma 20.(1) in $\Gamma_L(A)$ liegen, gilt das auch für ihre Determinante d. Insgesamt ist also

$$d \;\in\; K \cap \Gamma_L(A) \;=\; \Gamma_K(A) \;=\; A\,,$$

da A als ganzabgeschlossen vorausgesetzt wurde.

Aufgabe 16

Ad (1).

Fall $d \equiv_4 2$ *oder* $d \equiv_4 3$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\sqrt{d}]$; cf. Aufgabe 3. Also ist eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\sqrt{d}}$ gegeben durch $(1, \sqrt{d})$. Das nichttriviale Element von $\mathrm{Gal}(\mathbf{Q}(\sqrt{d})|\mathbf{Q})$ schickt $\sqrt{d}$ auf $-\sqrt{d}$. Nach Bemerkung 25 ist also

$$\Delta_{\mathbf{Q}(\sqrt{d})} \;=\; (\sqrt{d} - (-\sqrt{d}))^2 \;=\; 4d\,.$$

Fall $d \equiv_4 1$. Schreibe $\alpha := \frac{1}{2}(1 + \sqrt{d})$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Also ist eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\sqrt{d}}$ gegeben durch $(1, \alpha)$. Das nichttriviale Element von $\mathrm{Gal}(\mathbf{Q}(\sqrt{d})|\mathbf{Q})$ schickt $\sqrt{d}$ auf $-\sqrt{d}$ und also α auf $1 - \alpha$. Nach Bemerkung 25 ist also

$$\Delta_{\mathbf{Q}(\sqrt{d})} \;=\; (\alpha - (1 - \alpha))^2 \;=\; d\,.$$

Ad (2). Es ist $\mathbf{Q}(\sqrt{3}, \sqrt{13})|\mathbf{Q}$ ein Kompositum von $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$ und $\mathbf{Q}(\sqrt{13})|\mathbf{Q}$; cf. Definition 39, Beispiel 41.(1).

Es ist $\sqrt{3} \notin \mathbf{Q}(\sqrt{13})$, da $(a + b\sqrt{13})^2 = 3$ mit $a \in \mathbf{Q}$ und $b \in \mathbf{Q}$ mittels Koeffizientenvergleich bei 1 und $\sqrt{13}$ auf $a^2 + 13b^2 = 3$ und $2ab = 0$ führt, was weder für $a = 0$ noch für $b = 0$ lösbar ist. Also ist $[\mathbf{Q}(\sqrt{3}, \sqrt{13}) : \mathbf{Q}(\sqrt{13})] = 2$ und folglich $[\mathbf{Q}(\sqrt{3}, \sqrt{13}) : \mathbf{Q}] = 4$. Wegen

$$[\mathbf{Q}(\sqrt{3}, \sqrt{13}) : \mathbf{Q}] \;=\; 4 \;=\; [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \cdot [\mathbf{Q}(\sqrt{13}) : \mathbf{Q}]$$

sind $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$ und $\mathbf{Q}(\sqrt{13})|\mathbf{Q}$ linear disjunkt.

Mit (1) sind $\Delta_{\mathbf{Q}(\sqrt{3})} = 12$ und $\Delta_{\mathbf{Q}(\sqrt{13})} = 13$ teilerfremd. Mittels Satz 48.(2) erhalten wir also

$$\Delta_{\mathbf{Q}(\sqrt{3},\sqrt{13})} \;=\; (\Delta_{\mathbf{Q}(\sqrt{3})})^{[\mathbf{Q}(\sqrt{13}):\mathbf{Q}]} \cdot (\Delta_{\mathbf{Q}(\sqrt{13})})^{[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]} \;=\; 12^2 \cdot 13^2 \;=\; 2^4 \cdot 3^2 \cdot 13^2\,.$$

Es ist übrigens dank Satz 48.(1) auch $\mathcal{O}_{\mathbf{Q}(\sqrt{3},\sqrt{13})} = \mathbf{Z}[\sqrt{3}, \frac{1}{2}(1 + \sqrt{13})]$.

Aufgabe 17

Vorbemerkung. Sei K ein Körper. Wir haben die K-lineare Abbildung des *formalen Ableitens*

$$\begin{array}{rcll} K[X] & \longmapsto & K[X] & \\ 1 & \longmapsto & 0 & \\ X^s & \longmapsto & sX^{s-1} & \text{für } s \geqslant 1 \\ u(X) & \longmapsto & u'(X) & \end{array}$$

Für $u(X)$, $v(X) \in K[X]$ ist $(u(X)v(X))' = u'(X)v(X) + u(X)v'(X)$. Denn beide Seiten sind K-linear in $u(X)$ und in $v(X)$; und die Gleichung trifft zu für $u(X) = X^s$ und $v(X) = X^t$ für $s, t \geqslant 0$: o.E. ist $s, t \geqslant 1$, und dann ist

$$(X^{s+t})' \;=\; (s+t)X^{s+t-1} \;=\; sX^{s-1} \cdot X^t + X^s \cdot tX^{t-1} \;=\; (X^s)'X^t + X^s(X^t)' \,.$$

Cf. [**5,** Aufgabe 9].

Ad (1). Wir erinnern an $\zeta_n = \exp(2\pi\mathrm{i}/n)$.

Wir kürzen $f(X) := \mu_{\zeta_n\,,\mathbf{Q}}(X)$ ab. Dank Aufgabe 2.(8) liegt $f(X) \in \mathbf{Z}[X]$. Da $\zeta_n^n - 1 = 0$, ist $f(X)$ ein Teiler von $X^n - 1$ in $\mathbf{Q}[X]$; also auch in $\mathbf{Z}[X]$, wie Polynomdivision zeigt.

Wir *behaupten,* daß für $k \in \mathbf{Z}$ mit k teilerfremd zu n durch $\zeta_n \mapsto \zeta_n^k$ ein Automorphismus von $\mathbf{Q}(\zeta_n)$ definiert wird, der auf $\mathbf{Q}$ ohnehin identisch einschränkt; cf. [**5,** §2.3.4].

Es ist dazu zu zeigen, daß $f(\zeta_n^k) = 0$ ist.

Zerlege $k = p_1 p_2 \cdots p_\ell$ mit $\ell \geqslant 0$ und $p_i > 0$ prim für $i \in [1, \ell]$. Es genügt, für jede Nullstelle ζ von $f(X)$ in $\mathbf{Q}(\zeta_n)$ zu zeigen, daß auch $f(\zeta^{p_i}) \stackrel{!}{=} 0$ ist für alle $i \in [1, \ell]$.

Als irreduzibles normiertes Polynom in $\mathbf{Q}[X]$ mit Nullstelle ζ ist dann auch $f(X) = \mu_{\zeta\,,\mathbf{Q}}(X)$.

Sei $p > 0$ prim und kein Teiler von n. Es genügt, $f(\zeta^p) \stackrel{!}{=} 0$ zu zeigen. Sei $g(X) := \mu_{\zeta^p\,,\mathbf{Q}}(X)$. Es sind $f(X)$ und $g(X)$ Teiler von $X^n - 1$ in $\mathbf{Z}[X]$, da $\zeta^n = 1$ und $(\zeta^p)^n = 1$.

Es genügt, $f(X) \stackrel{!}{=} g(X)$ zu zeigen. *Annahme,* $f(X) \neq g(X)$. Dann sind $f(X)$ und $g(X)$ zwei verschiedene irreduzible Teiler von $X^n - 1$. Da $\mathbf{Q}[X]$ ein Hauptidealbereich ist, cf. [**5,** §1.7.4], sind $f(X)$ und $g(X)$ Primelemente von $\mathbf{Q}[X]$, die beide in der Primfaktorzerlegung von $X^n - 1$ in $\mathbf{Q}[X]$ im Sinne von Aufgabe 2.(3) als Faktor auftreten. Also teilt auch $f(X)g(X)$ das Polynom $X^n - 1$ in $\mathbf{Q}[X]$; also auch in $\mathbf{Z}[X]$, wie Polynomdivision zeigt. Sei $h(X) \in \mathbf{Z}[X]$ normiert mit $f(X)g(X)h(X) = X^n - 1$.

Für ein Polynom $u(X) \in \mathbf{Z}[X]$ schreiben wir $\bar{u}(X) \in \mathbf{F}_p[X]$ für sein durch koeffizientenweise Anwendung des Restklassenmorphismus $\mathbf{Z} \to \mathbf{F}_p$ erhaltenes Bild.

Es ist $\bar{f}(X)\bar{g}(X)\bar{h}(X) = X^n - 1$ in $\mathbf{F}_p[X]$; cf. [**5,** §1.6.2].

Da $g(\zeta^p) = 0$ ist, ist ζ eine Nullstelle von $g(X^p)$. Folglich ist $f(X)$ ein Teiler von $g(X^p)$ in $\mathbf{Z}[X]$. Also ist $\bar{f}(X)$ ein Teiler von $\bar{g}(X)^p = \bar{g}(X^p)$ in $\mathbf{F}_p[X]$.

Sei ein normiertes Polynom $a(X) \in \mathbf{Z}[X]$ von Grad $\geqslant 1$ so gewählt, daß $\bar{a}(X)$ ein irreduzibler Teiler von $\bar{f}(X)$ ist. Da auch $\mathbf{F}_p[X]$ ein Hauptidealbereich ist, cf. [**5,** §1.7.4], folgt aus der Tatsache, daß das Primelement $\bar{a}(X)$ in der Primfaktorzerlegung von $\bar{g}(X)^p$ im Sinne von Aufgabe 2.(3) als Faktor auftaucht, daß es auch in der Primfaktorzerlegung von $\bar{g}(X)$ als Faktor auftaucht. Da $\bar{a}(X)$ ein Teiler von $\bar{f}(X)$ und von $\bar{g}(X)$ ist, teilt nun $\bar{a}(X)^2$ das Polynom $X^n - 1$ in $\mathbf{F}_p[X]$.

Schreibe $X^n - 1 = \bar{a}(X)^2\,\bar{b}(X)$ mit einem geeigneten normierten Polynom $b(X) \in \mathbf{Z}[X]$. Formales Ableiten beider Seiten gibt

$$\begin{aligned} nX^{n-1} &= (X^n - 1)' \\ &= (\bar{a}(X)^2\bar{b}(X))' \\ &= \bar{a}'(X)\bar{a}(X)\bar{b}(X) + \bar{a}(X)\bar{a}'(X)\bar{b}(X) + \bar{a}(X)\bar{a}(X)\bar{b}'(X) \\ &= \bar{a}(X)(2\bar{a}'(X)b(X) + a(X)b'(X)) \,. \end{aligned}$$

Da p kein Teiler von n ist, folgt, daß $\bar{a}(X)$ in der Primfaktorzerlegung von X^{n-1} als Faktor auftritt. Somit folgt $\bar{a}(X) = X$ und also $X^n - 1 = X^2\bar{b}(X)$ in $\mathbf{F}_p[X]$. Der konstante Term der linken Seite ist -1, der der rechten ist 0. *Widerspruch.* Dies zeigt die *Behauptung.*

Somit existiert für $k \in \mathbf{Z}$ mit k teilerfremd zu n der Körpermorphismus $\sigma_k : \mathbf{Q}(\zeta_n) \to \mathbf{Q}(\zeta_n)$, $\zeta_n \mapsto \zeta_n^k$; cf. [**5,** §2.4.3]. Ferner ist für $k, \ell \in \mathbf{Z}$ teilerfremd zu n genau dann $\sigma_k = \sigma_\ell$, wenn $\zeta_n^k = \zeta_n^\ell$ ist, i.e. wenn

$k + (n) = \ell + (n)$ ist. Dies gibt die Wohldefiniertheit und die Injektivität der Abbildung

$$\begin{array}{rcl} \mathrm{U}(\mathbf{Z}/(n)) & \longrightarrow & \mathrm{Aut}(\mathbf{Q}(\zeta_n)|\mathbf{Q}) \\ k + (n) & \longmapsto & \sigma_k \ . \end{array}$$

Wir *behaupten* die Surjektivität dieser Abbildung. Da $|\{\, \zeta_n^k \,:\, k \in [0, n-1] \,\}| = n$ ist, da jede Potenz von ζ_n eine Nullstelle von $X^n - 1$ in $\mathbf{Q}(\zeta_n)$ ist und da $X^n - 1$ dort nicht mehr als n verschiedene Nullstellen haben kann, ist jede Nullstelle von $X^n - 1$ auch eine Potenz von ζ_n , mit Exponent in $[0, n-1]$. Folglich ist

$$X^n - 1 \ = \prod_{k \in [0, n-1]} (X - \zeta_n^k) \ \in \ \mathbf{Q}(\zeta_n)[X] \ .$$

Für $\alpha \in \mathrm{Aut}(\mathbf{Q}(\zeta_n)|\mathbf{Q})$ ist auch $\alpha(\zeta_n)$ wieder eine Nullstelle von $X^n - 1$. Es ist also $\alpha(\zeta_n) = \zeta_n^k$ für ein $k \in [0, n-1]$. *Wäre* k nicht teilerfremd zu n, dann hätten k und n einen gemeinsamen Teiler $d \in \mathbf{Z}_{>1}$, und es wäre $(\zeta_n^k)^{n/d} = (\zeta_n^n)^{k/d} = 1$, aber $\alpha^{-1}((\zeta_n^k)^{n/d}) = \zeta_n^{n/d} \neq 1$, was *nicht* sein kann. Also ist k teilerfremd zu n und $\alpha = \sigma_k$. Dies zeigt die *Behauptung.*

Sodann ist für $k, \ell \in \mathbf{Z}$ teilerfremd zu n auch

$$(\sigma_k \circ \sigma_\ell)(\zeta_n) \ = \ \sigma_k(\zeta_n^\ell) \ = \ \zeta_n^{\ell k} \ = \ \sigma_{k\ell}(\zeta_n) \ ,$$

somit $\sigma_k \circ \sigma_\ell = \sigma_{k\ell}$ und also unsere Abbildung ein Gruppenmorphismus.

Schließlich ist wegen $X^n - 1 = \prod_{k \in [0, n-1]} (X - \zeta_n^k)$ der Körper $\mathbf{Q}(\zeta_n)$ bereits Zerfällungskörper von $X^n - 1 \in \mathbf{Q}[X]$; cf. **[5,** §2.5.1]. Es zerfällt $X^n - 1$ in $\mathbf{Q}[X]$ in verschiedene normierte irreduzible Faktoren, da ein normierter irreduzibler Faktor von $X^n - 1$ in $\mathbf{Q}[X]$ mit Exponent $\geqslant 2$ einen Linearfaktor von $X^n - 1$ in $\mathbf{Q}(\zeta_n)[X]$ mit Exponent $\geqslant 2$ nach sich zöge, den es aber nicht gibt. Als Zerfällungskörper eines Polynoms ist $\mathbf{Q}(\zeta_n)|\mathbf{Q}$ galoisch; cf. **[5,** §3.5.1.4].

Ad (2). Für $d \in \mathbf{Z}_{\geqslant 1}$ mit $n \equiv_d 0$ ist $\Phi_d(X)$ ein irreduzibler normierter Teiler von $X^n - 1$ falls $n \equiv_d 0$, da dann $\zeta_d^n - 1 = (\zeta_d^d)^{n/d} - 1 = 0$ ist.

Es zerfällt $X^n - 1$ in $\mathbf{Q}[X]$ in ein Produkt paarweise verschiedener irreduzibler Faktoren, wie bereits in (1) angemerkt.

Hierzu hätte man auch anführen können, daß $X^n - 1$ und $(X^n - 1)' = nX^{n-1}$ in $\mathbf{Q}[X]$ teilerfremd sind.

Es bleibt zu zeigen, daß jeder normierte irreduzible Faktor $a(X)$ von $X^n - 1$ in $\mathbf{Q}[X]$ von der Form $\Phi_d(X)$ ist für einen Teiler $d \in \mathbf{Z}_{\geqslant 1}$ von n, i.e. daß $a(\zeta_d) = 0$ ist.

Dank $X^n - 1 = \prod_{k \in [0, n-1]} (X - \zeta_n^k)$ aus (1) gibt es ein $k \in [0, n-1]$ mit $a(\zeta_n^k) = 0$. Sei g der größte gemeinsame Teiler von n und k. Schreibe $k = sg$ mit $s \in \mathbf{Z}$. Dann ist s teilerfremd zu n. Sei $d := n/g$. Mit ζ_n^k ist auch $\sigma_s^{-1}(\zeta_n^k) \ = \ \sigma_s^{-1}(\zeta_n^s)^g \ = \ \zeta_n^g = \zeta_{dg}^g = \zeta_d$ eine Nullstelle von $a(X)$.

Aufgabe 18

Schreibe $n := [K : \mathbf{Q}]$.

Ad (1). Gemäß Lemma 33 ist $\mathcal{O}_K$ eine $\mathbf{Z}$-Ordnung.

Sei C eine $\mathbf{Z}$-Ordnung in K. Sei $c \in C$. Wir haben $c \overset{!}{\in} \mathcal{O}_K$ zu zeigen. Dies folgt aus Lemma 1.$(3 \Rightarrow 1)$, da $\mathbf{Z}[c] \subseteq C$ liegt und C ein endlich erzeugter $\mathbf{Z}$-Modul ist.

Ad (2). Sei $G = {}_{\mathbf{Z}}\langle\, y_1 \,,\, \ldots \,,\, y_n \,\rangle$. Es ist $G^\# = {}_{\mathbf{Z}}\langle\, y_1' \,,\, \ldots \,,\, y_n' \,\rangle$, mit $y_i' \in K$ für $i \in [1, n]$ so, daß $\mathrm{Tr}_{K|\mathbf{Q}}(y_i \cdot y_j') = \partial_{i,\,j}$ für $j \in [1, n]$; cf. Lemma 31.(3).

Sei $H = {}_{\mathbf{Z}}\langle\, z_1 \,,\, \ldots \,,\, z_n \,\rangle$. Es ist $H^\# = {}_{\mathbf{Z}}\langle\, z_1' \,,\, \ldots \,,\, z_n' \,\rangle$, mit $z_i' \in K$ für $i \in [1, n]$ so, daß $\mathrm{Tr}_{K|\mathbf{Q}}(z_i \cdot z_j') = \partial_{i,\,j}$ ist für $j \in [1, n]$.

Schreibe $y_i = \sum_{j\in[1,n]} z_j\, b_{j,i}$ für $i \in [1,n]$, wobei $B := (b_{i,\,j})_{i,\,j} \in \mathbf{Z}^{n\times n}$.

Es ist $B \in \mathrm{GL}_n(\mathbf{Q})$ und somit $\det(B) \in \mathbf{Z}^\times$.

Wir *behaupten,* daß für $i \in [1,n]$

$$z'_i \stackrel{!}{=} \sum_{j\in[1,n]} b_{i,\,j}\, y'_j$$

ist. Für $k \in [1,n]$ wird auf der einen Seite

$$\mathrm{Tr}_{K|\mathbf{Q}}(z'_i \cdot y_k) \;=\; \textstyle\sum_{j\in[1,n]} \mathrm{Tr}_{K|\mathbf{Q}}(z'_i \cdot z_j) b_{j,k} \;=\; \sum_{j\in[1,n]} \partial_{i,\,j}\, b_{j,k} \;=\; b_{i,k}\;,$$

auf der anderen Seite

$$\mathrm{Tr}_{K|\mathbf{Q}}(\textstyle\sum_{j\in[1,n]} b_{i,\,j}\, y'_j \cdot y_k) \;=\; \sum_{j\in[1,n]} b_{i,\,j}\; \mathrm{Tr}_{K|\mathbf{Q}}(y'_j\, y_k) \;=\; \sum_{j\in[1,n]} b_{i,\,j}\, \partial_{j,k} \;=\; b_{i,k}\;,$$

also beidesmal dasselbe. Dies zeigt die *Behauptung.*

Folglich ist $|H/G| = |\det(B)|$ und $|G^\#/H^\#| = |\det(B)|$; cf. Aufgabe 14.(2).

Insbesondere ist $|H/G| = |G^\#/H^\#|$.

Ad (3). Nach (1) ist $R \subseteq \mathcal{O}_K$. Also ist

$$R \;\subseteq\; \mathcal{O}_K \;\subseteq\; \mathcal{O}_K^\# \;\subseteq\; R^\#\;;$$

cf. Bemerkung 30.

Es ist $|\Delta_{K|\mathbf{Q},\,\underline{y}}| \stackrel{\text{A. 14.(3)}}{=} |R^\#/R|$, was folglich in $\mathbf{Z}_{\geqslant 1}$ liegt; cf. Lemmata 22 und 20.(2).

Es ist die abelsche Gruppe $\mathcal{O}_K^\#/\mathcal{O}_K$ isomorph zur abelschen Gruppe $(\mathcal{O}_K^\#/R)/(\mathcal{O}_K/R)$.

Es liegt $\mathcal{O}_K^\#/R \leqslant R^\#/R$ und ist mithin endlich. Also ist $|\mathcal{O}_K^\#/R| = |\mathcal{O}_K^\#/\mathcal{O}_K| \cdot |\mathcal{O}_K/R|$.

Genauso sieht man $|R^\#/R| = |R^\#/\mathcal{O}_K^\#| \cdot |\mathcal{O}_K^\#/R|$.

Insgesamt ist also

$$|\Delta_{K|\mathbf{Q},\,\underline{y}}| \;=\; |R^\#/R| \;=\; |R^\#/\mathcal{O}_K^\#| \cdot |\mathcal{O}_K^\#/\mathcal{O}_K| \cdot |\mathcal{O}_K/R| \;\stackrel{(2)}{=}\; |\mathcal{O}_K^\#/\mathcal{O}_K| \cdot |\mathcal{O}_K/R|^2\;,$$

und diese Zahl ist nach Voraussetzung quadratfrei. Also ist $|\mathcal{O}_K/R| = 1$, i.e. $R = \mathcal{O}_K$.

Ad (4).

> Nach Aufgabenstellung dürfen wir als bekannt voraussetzen, daß $X^3 + X + 1 \in \mathbf{Q}[X]$ ein irreduzibles Polynom ist.
>
> *Wäre* es reduzibel, dann würde es in zwei normierte Faktoren in $\mathbf{Z}[X]$ von Grad $\geqslant 1$ zerfallen; cf. Aufgabe 2.(7). Dann aber würde auch $X^3 + X + 1 \in \mathbf{F}_2[X]$ in zwei normierte Faktoren in $\mathbf{Z}[X]$ von Grad $\geqslant 1$ zerfallen. Diese ist aber mangels Nullstelle in $\mathbf{F}_2$ *nicht* möglich.

Schreibe $\mathrm{Tr} := \mathrm{Tr}_{K|\mathbf{Q}}$. Berechnen wir zunächst bezüglich der $\mathbf{Q}$-linearen Basis $\underline{y} := (\alpha^0, \alpha^1, \alpha^2)$ von K

$$\begin{array}{lcll} \mathrm{Tr}(1) & = & \mathrm{tr}\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) & = \quad 3 \\ \mathrm{Tr}(\alpha) & = & \mathrm{tr}\left(\begin{smallmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{smallmatrix}\right) & = \quad 0 \\ \mathrm{Tr}(\alpha^2) & = & \mathrm{tr}\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & 0 & -1 \end{smallmatrix}\right) & = \quad -2 \end{array}$$

Schreibe $\mathrm{Tr} := \mathrm{Tr}_{K|\mathbf{Q}}$. Es wird

$$\begin{aligned}\Delta_{K|\mathbf{Q},\,\underline{y}} &= \det\begin{pmatrix}\mathrm{Tr}(\alpha^0\cdot\alpha^0) & \mathrm{Tr}(\alpha^0\cdot\alpha^1) & \mathrm{Tr}(\alpha^0\cdot\alpha^2)\\ \mathrm{Tr}(\alpha^1\cdot\alpha^0) & \mathrm{Tr}(\alpha^1\cdot\alpha^1) & \mathrm{Tr}(\alpha^1\cdot\alpha^2)\\ \mathrm{Tr}(\alpha^2\cdot\alpha^0) & \mathrm{Tr}(\alpha^2\cdot\alpha^1) & \mathrm{Tr}(\alpha^2\cdot\alpha^2)\end{pmatrix}\\ &= \det\begin{pmatrix}\mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2)\\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(-\alpha-1)\\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(-\alpha-1) & \mathrm{Tr}(-\alpha^2-\alpha)\end{pmatrix} = \det\begin{pmatrix}3 & 0 & -2\\ 0 & -2 & -3\\ -2 & -3 & 2\end{pmatrix} = -31\end{aligned}$$

eine quadratfreie ganze Zahl.

Dank (3) ist also die $\mathbf{Z}$-Ordnung $\mathbf{Z}[\alpha] = {}_{\mathbf{Z}}\langle\underline{y}\rangle$ gleich $\mathcal{O}_K$.

Dies hat insbesondere zur Folge, daß $\underline{y}$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_K$ und somit $\Delta_K = \Delta_{K|\mathbf{Q},\,\underline{y}} = -31$ ist.

Aufgabe 19

Ad (1). Beachte $\delta^3 = 2$.

Es ist $(1, \delta, \delta^2)$ eine $\mathbf{Z}$-lineare Basis von $\mathbf{Z}[\delta]$. Es ist

$$(\mathrm{Gram}_{\mathbf{Q}(\delta)|\mathbf{Q},(1,\delta,\delta^2)})^{-1} = \begin{pmatrix}3&0&0\\0&0&6\\0&6&0\end{pmatrix}^{-1} = \tfrac{1}{6}\begin{pmatrix}2&0&0\\0&0&1\\0&1&0\end{pmatrix} ;$$

cf. Beispiel 26.(2). Also ist die zu $(1, \delta, \delta^2)$ duale Basis gegeben durch $(\frac{1}{3}, \frac{1}{6}\delta^2, \frac{1}{6}\delta)$. Also ist

$$\mathbf{Z}[\delta]^{\#} = {}_{\mathbf{Z}}\langle\tfrac{1}{3}, \tfrac{1}{6}\delta^2, \tfrac{1}{6}\delta\rangle .$$

Ad (2). Da $\delta \in \mathcal{O}_{\mathbf{Q}(\delta)}$ wegen $\mu_{\delta,\mathbf{Q}}(X) = X^3 - 2 \in \mathbf{Z}[X]$, ist $\mathbf{Z}[\delta] \subseteq \mathcal{O}_{\mathbf{Q}(\delta)} \subseteq \mathcal{O}^{\#}_{\mathbf{Q}(\delta)} \subseteq \mathbf{Z}[\delta]^{\#}$; cf. Bemerkung 30, Lemma 31.(2).

Es genügt also, für $x := s_0 + s_1\delta + s_2\delta^2 \in \mathcal{O}_{\mathbf{Q}(\delta)}$ mit $s_0 \in \frac{1}{3}\mathbf{Z}$, $s_1 \in \frac{1}{6}\mathbf{Z}$, $s_2 \in \frac{1}{6}\mathbf{Z}$ nachzuweisen, daß $x \overset{!}{\in} \mathbf{Z}[\delta]$ liegt.

Es ist auch

$$\mathbf{Z}[\delta]^{\#} \supseteq \mathcal{O}_{\mathbf{Q}(\delta)} \ni x^2 = (s_0^2 + 4s_1s_2) + (2s_2^2 + 2s_0s_1)\delta + (s_1^2 + 2s_0s_2)\delta^2 .$$

Da $s_1^2 + 2s_0s_2 \in \frac{1}{6}\mathbf{Z}$ und $2s_0s_2 \in \frac{1}{9}\mathbf{Z}$ liegen, ist auch $s_1^2 \in \frac{1}{18}\mathbf{Z}$ und somit $s_1 \in \frac{1}{3}\mathbf{Z}$.

Es genügt also, für $x := s_0 + s_1\delta + s_2\delta^2 \in \mathcal{O}_{\mathbf{Q}(\delta)}$ mit $s_0 \in \frac{1}{3}\mathbf{Z}$, $s_1 \in \frac{1}{3}\mathbf{Z}$, $s_2 \in \frac{1}{6}\mathbf{Z}$ nachzuweisen, daß $x \overset{!}{\in} \mathbf{Z}[\delta]$ liegt.

Es ist

$$\mathbf{Z}[\delta]^{\#} \supseteq \mathcal{O}_{\mathbf{Q}(\delta)} \ni x^3 = (s_0^3+2s_1^3+4s_2^3+12s_0s_1s_2)+3(s_0^2s_1+2s_1^2s_2+2s_2^2s_0)\delta+3(s_0^2s_2+s_1^2s_0+2s_2^2s_1)\delta^2 .$$

Es ist $s_0^3 + 2s_1^3 + 4s_2^3 + 12s_0s_1s_2 \in \frac{1}{3}\mathbf{Z}$, und dabei ist $s_0^3 \in \frac{1}{27}\mathbf{Z}$, $2s_1^3 \in \frac{1}{27}\mathbf{Z}$ und $12s_0s_1s_2 \in \frac{1}{9}\mathbf{Z}$. Folglich ist $s_2^3 \in \frac{1}{4\cdot 27}\mathbf{Z}$ und somit $s_2 \in \frac{1}{3}\mathbf{Z}$.

Also ist $\mathcal{O}_{\mathbf{Q}(\delta)} \subseteq \frac{1}{3}\mathbf{Z}[\delta]$.

Es genügt also, für $x := s_0 + s_1\delta + s_2\delta^2 \in \mathcal{O}_{\mathbf{Q}(\delta)}$ mit $x \in \frac{1}{3}\mathbf{Z}[\delta]$ nachzuweisen, daß $x \overset{!}{\in} \mathbf{Z}[\delta]$ liegt.

Schreibe $3s_i =: t_i \in \mathbf{Z}$ für $i \in \{0, 1, 2\}$. Wir haben zu zeigen, daß $t_i \overset{!}{\equiv}_3 0$ ist für $i \in \{0, 1, 2\}$.

Es ist

$$0 \equiv_9 t_0^3 + 2t_1^3 + 4t_2^3 + 12t_0t_1t_2 \equiv_3 t_0 + 2t_1 + 4t_2 \equiv_3 t_0 - t_1 + t_2 .$$

Schreibe $t_2 =: t_1 - t_0 + 3u$ mit $u \in \mathbf{Z}$.

Aus $x^2 \in \mathcal{O}_{\mathbf{Q}(\delta)} \subseteq \frac{1}{3}\mathbf{Z}[\delta]$ folgt nun

$$0 \equiv_3 t_0^2 + 4t_1t_2 \equiv_3 t_0^2 + 4t_1(t_1 - t_0) \equiv_3 t_0^2 + 2t_0t_1 + t_1^2 = (t_0 + t_1)^2$$

und also $0 \equiv_3 t_0 + t_1$. Schreibe $t := t_0$ und $t_1 =: -t + 3v$ mit $v \in \mathbf{Z}$. Schreibe $w := u + v \in \mathbf{Z}$. Dann ist $t_2 = t_1 - t_0 + 3u = -2t + 3w$.

Es bleibt $t \overset{!}{\equiv}_3 0$ zu zeigen.

Es ist

$$\tfrac{1}{3}\mathbf{Z}[\delta] \supseteq \mathcal{O}_{\mathbf{Q}(\delta)} \ni x^4 = (s_0^4 + 24s_0^2s_1s_2 + 8s_0s_1^3 + 16s_0s_2^3 + 24s_1^2s_2^2) + \underbrace{(\dots)}_{\in \mathbf{Q}}\delta + \underbrace{(\dots)}_{\in \mathbf{Q}}\delta^2 .$$

Also ist

$$\begin{aligned} 0 &\equiv_{27} t_0^4 + 24t_0^2t_1t_2 + 8t_0t_1^3 + 16t_0t_2^3 + 24t_1^2t_2^2 \\ &= 9t^4 - 648t^3v + 216t^3w + 648t^2v^2 + 1944t^2vw - 648t^2w^2 \\ &\quad + 216tv^3 - 2592tv^2w - 1296tvw^2 + 432tw^3 + 1944v^2w^2 \\ &\equiv_{27} 9t^4 . \end{aligned}$$

Es folgt $t^4 \equiv_3 0$, also $t \equiv_3 0$.

> Einfachere Lösungen werden gerne entgegengenommen. Einen systematischen Zugang findet man e.g. in **[4,** §4.5.4].

Schließlich wird dank Beispiel 26.(2) nun $\Delta_{\mathbf{Q}(\delta)} = \Delta_{\mathbf{Q}(\delta)|\mathbf{Q},\,(1,\delta,\delta^2)} = -2^2 \cdot 3^3$.

Aufgabe 20

Aus (2) folgt (1), ausgenommen zunächst die Surjektivitiät von α. Aber es enthält dann $\alpha(L)$ sowohl $\alpha(\varphi'(L')) = \tilde{\varphi}'(L')$ als auch $\alpha(\varphi''(L'')) = \tilde{\varphi}''(L'')$, sodaß $\alpha(L) = \tilde{L}$ zu sein hat. Also folgt auch die Surjektivität von α.

Ad (2).

Zur Eindeutigkeit.

Seien $\beta : L \to M$ mit $\beta \circ \varphi' = \psi'$ und $\beta \circ \varphi'' = \psi''$ und $\tilde{\beta} : L \to M$ mit $\tilde{\beta} \circ \varphi' = \psi'$ und $\tilde{\beta} \circ \varphi'' = \psi''$ gegeben. Wir haben $\beta \overset{!}{=} \tilde{\beta}$ zu zeigen. Betrachte $F := \{\, y \in L : \beta(y) = \tilde{\beta}(y) \,\}$. Es ist F ein Teilkörper von L, da $1 \in F$ und da für $y, z \in F$ auch $\beta(y - z) = \beta(y) - \beta(z) = \tilde{\beta}(y) - \tilde{\beta}(z) = \tilde{\beta}(y - z)$, i.e. $y - z \in F$, und $\beta(yz) = \beta(y) \cdot \beta(z) = \tilde{\beta}(y) \cdot \tilde{\beta}(z) = \tilde{\beta}(yz)$, i.e. $yz \in F$ ist. Es ist $\varphi'(L') \subseteq F$, da für $y' \in L'$ sich $\beta(\varphi'(y')) = \psi'(y') = \tilde{\beta}(\varphi'(y'))$ ergibt. Ebenso ist $\varphi''(L'') \subseteq F$. Da $L|K$ Kompositum von $L'|K$ und $L''|K$ ist via ψ', ψ'', ist L der einzige Teilkörper von L, der $\varphi'(L')$ und $\varphi''(L'')$ enthält. Somit folgt $F = L$, i.e. $\beta = \tilde{\beta}$.

Zur Existenz.

Schreibe $L' = K(z')$ mit $z' \in L'$ geeignet; cf. **[5,** Aufgabe 54]. Schreibe $w' := \varphi'(z')$. Es ist $\varphi'(L') = \varphi'(K(z')) = K(w')$.

Schreibe $L'' = K(z'')$ mit $z'' \in L''$ geeignet; cf. **[5,** Aufgabe 54]. Schreibe $w'' := \varphi''(z'')$. Es ist $\varphi''(L'') = \varphi''(K(z'')) = K(w'')$.

Da $L'|K$ und $L''|K$ linear disjunkt sind, ist $\mu_{z'',\,K}(X) \in L'[X]$ irreduzibel. Also ist auch $\mu_{z'',\,K}(X) = \mu_{w'',\,K}(X) \in \varphi'(L')[X] = K(w')[X]$ irreduzibel. Mithin ist $\mu_{w'',\,K}(X) = \mu_{w'',\,K(w')}(X)$; cf. **[5,** §2.3].

Beachte noch $L = K(w', w'')$, da ein Teilkörper von L genau dann K, w' und w'' enthält, wenn er $K(w') = \varphi(L')$ und $K(w'') = \varphi(L'')$ enthält, i.e. wenn er gleich L ist, denn L ist ein Kompositum via φ' und φ''.

Schreibe $\tilde{\varphi}' := (\varphi'|^{K(w')})^{-1} : K(w') \to L'$, $w' \mapsto z'$.

Wir haben den Körpermorphismus $\psi' \circ \tilde{\varphi}' : K(w') \to M$.

Es ist

$$\mu^{\psi' \circ \tilde{\varphi}'}_{w'', K'(w')}(X) \;=\; \mu^{\psi' \circ \tilde{\varphi}'}_{w'', K}(X) \;=\; \mu_{w'', K}(X) \;=\; \mu_{z'', K}(X) \;=\; \mu_{\psi''(z''), K}(X)\,;$$

cf. **[5,** §1.6.2]. Also ist

$$\mu^{\psi' \circ \tilde{\varphi}'}_{w'', K(w')}(\psi''(z'')) \;=\; \mu_{\psi''(z''), K}(\psi''(z'')) \;=\; 0\,.$$

Folglich gibt es einen Körpermorphismus $\beta : L = K(w')(w'') \to M$ mit $\beta|_{K(w')} = \psi' \circ \tilde{\varphi}'$ und $\beta(w'') = \psi''(z'')$; cf. **[5,** §2.3.4].

Für $y' \in L'$ ist $\beta(\varphi'(y')) = (\psi' \circ \tilde{\varphi}')(\varphi'(y')) = \psi'(y')$. Also ist $\beta \circ \varphi' = \psi'$. Speziell ist $\beta|^K_K = \mathrm{id}_K$.

Ferner ist $\beta(\varphi''(z'')) = \beta(w'') = \psi''(z'')$. Da $L'' = K(z'')$, folgt $\beta \circ \varphi'' = \psi''$. ▫

Man kann auch anführen, daß im linear disjunkten Fall für ein Kompositum $L|K$ von $L'|K$ und $L''|K$, mit φ' und φ'', ein Isomorphismus von K-Algebren $L' \otimes_K L'' \to L$, $u' \otimes u'' \mapsto \varphi'(u') \cdot \varphi''(u'')$ existiert, surjektiv nach Konstruktion und dann injektiv wegen Dimension.

Aufgabe 21

O.E. ist $m,\, n \geqslant 1$.

Behauptung. Es ist $\det(B)$ unabhängig von der Wahl von α.

Sei $\beta : [1, mn] \xrightarrow{\sim} [1, m] \times [1, n]$, $k \mapsto \beta(k) =: (\beta'(k), \beta''(k))$ eine eine weitere Bijektion. Sei $\varphi \in \mathrm{S}_{mn}$ definiert durch $\varphi := \alpha^{-1} \circ \beta$.

Für $k \in [1, mn]$ wird $(\alpha'(\varphi(k)), \alpha''(\varphi(k))) = \alpha(\varphi(k)) = \beta(k) = (\beta'(k), \beta''(k))$. Somit wird

$$\begin{aligned}
\det((a_{\beta'(k),\beta'(\ell)}\partial_{\beta''(k),\beta''(\ell)})_{k,\ell}) &= \det((a_{\alpha'(\varphi(k)),\alpha'(\varphi(\ell))}\partial_{\alpha''(\varphi(k)),\alpha''(\varphi(\ell))})_{k,\ell}) \\
&= \mathrm{sgn}(\varphi)\det((a_{\alpha'(k),\alpha'(\varphi(\ell))}\partial_{\alpha''(k),\alpha''(\varphi(\ell))})_{k,\ell}) \\
&= \mathrm{sgn}(\varphi)^2\det((a_{\alpha'(k),\alpha'(\ell)}\partial_{\alpha''(k),\alpha''(\ell)})_{k,\ell}) \\
&= \det((a_{\alpha'(k),\alpha'(\ell)}\partial_{\alpha''(k),\alpha''(\ell)})_{k,\ell})\,.
\end{aligned}$$

Dies zeigt die *Behauptung.*

Für $k \in \mathbf{Z}$ sei $\overline{k} \in [0, m-1]$ und $\underline{k} \in \mathbf{Z}$ mit $k = \underline{k}m + \overline{k}$. I.e. Division von k durch m gibt $\underline{k}$ mit Rest $\overline{k}$.

Unter Verwendung unserer Behauptung können wir nun o.E. die Bijektion

$$\begin{aligned}
[1, mn] &\xrightarrow[\sim]{\alpha} [1, m] \times [1, n] \\
k &\longmapsto (\overline{k-1}+1, \underline{k-1}+1) \\
(s-1)+(t-1)m+1 &\longmapsfrom (s, t)
\end{aligned}$$

wählen.

Dann wird $B := (a_{\overline{k-1}+1,\,\overline{\ell-1}+1}\partial_{\underline{k-1}+1,\,\underline{\ell-1}+1})_{k,\ell}$. Mit anderen Worten, es ist B die Blockdiagonalmatrix

$$B \;=\; \begin{pmatrix} A & & \\ & A & \\ & & \ddots \\ & & & A \end{pmatrix} \;\in\; K^{mn \times mn}\,.$$

Also ist $\det(B) = \det(A)^n$.

Aufgabe 22

Schreibe $n := [K : \mathbf{Q}]$. Sei $\underline{g}$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_K$.

Da $\Delta_{\mathbf{Q}} = 1$, ist o.E. $n \geqslant 2$.

Sei E ein Zerfällungskörper von $K|\mathbf{Q}$. Sei $U := \mathrm{Gal}(E|K) \leqslant \mathrm{Gal}(E|\mathbf{Q}) =: G$. Sei $G = \bigsqcup_{i\in[1,n]} \tau_i U$.

Es ist $\mathrm{S}_n = \mathrm{A}_n \sqcup (1,2)\mathrm{A}_n$. Seien

$$\begin{array}{rcl} P & := & \sum_{\varphi\in \mathrm{A}_n} \prod_{i\in[1,n]} \tau_i(g_{\varphi(i)}) \\ N & := & \sum_{\varphi\in (1,2)\mathrm{A}_n} \prod_{i\in[1,n]} \tau_i(g_{\varphi(i)}) \; . \end{array}$$

Also ist $\det(\mathrm{Vand}_{K|\mathbf{Q},\,\underline{g}}) = P - N$ und also $\Delta_K = \det(\mathrm{Vand}_{K|\mathbf{Q},\,\underline{g}})^2 = (P-N)^2 = (P+N)^2 - 4PN$.

Es genügt zu zeigen, daß $P + N$ und PN in $\mathbf{Z}$ liegen, da dann $(P+N)^2 \equiv_4 0$ oder $(P+N)^2 \equiv_4 1$, und jedenfalls $4PN \equiv_4 0$ ist.

Es genügt zu zeigen, daß $P + N$ und PN in $\mathbf{Q}$ liegen, da sie nach Konstruktion in $\mathcal{O}_E$ liegen, cf. Lemma 20.(1), und da $\mathcal{O}_E \cap \mathbf{Q} = \mathcal{O}_{\mathbf{Q}} = \mathbf{Z}$, cf. Bemerkung 8.(1).

Sei $\rho \in G$. Es genügt zu zeigen, daß $\rho(P+N) \stackrel{!}{=} P+N$ und $\rho(PN) \stackrel{!}{=} PN$ ist.

Es ist $G = \bigsqcup_{i\in[1,n]} \tau_i U = \bigsqcup_{j\in[1,n]} \rho\tau_j U$. Also gibt es ein $\psi \in \mathrm{S}_n$ mit $\rho\tau_j U = \tau_{\psi(j)} U$ für $j \in [1,n]$. So wird

$$\begin{array}{rcl} \rho(P) & = & \sum_{\varphi\in \mathrm{A}_n} \prod_{i\in[1,n]} (\rho\circ\tau_i)(g_{\varphi(i)}) \\ & = & \sum_{\varphi\in \mathrm{A}_n} \prod_{i\in[1,n]} \tau_{\psi(i)}(g_{\varphi(i)}) \\ & = & \sum_{\varphi\in \mathrm{A}_n} \prod_{j\in[1,n]} \tau_j(g_{\varphi\circ\psi^{-1}(j)}) \; , \end{array}$$

und genauso

$$\rho(N) \;=\; \sum_{\varphi\in (1,2)\mathrm{A}_n} \prod_{j\in[1,n]} \tau_j(g_{\varphi\circ\psi^{-1}(j)}) \; .$$

Fall $\psi \in \mathrm{A}_n$. Es ist $\rho(P) = P$ und $\rho(N) = N$, also auch $\rho(P+N) = P+N$ und $\rho(PN) = PN$.

Fall $\psi \in (1,2)\mathrm{A}_n$. Es ist $\rho(P) = N$ und $\rho(N) = P$, also auch $\rho(P+N) = P+N$ und $\rho(PN) = PN$.

Die Aussage dieser Aufgabe heißt Stickelbergscher Diskriminantensatz.

Aufgabe 23

Ad (1). Die Aussage ist falsch.

Sei etwa $K = \mathbf{Q}$, $L' = \mathbf{Q}(\sqrt[3]{2})$ und $L'' = \mathbf{Q}(\zeta_3)$. Sei $E' = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$; cf. Beispiel 10.(2). Sei $E'' := L''$, möglich, da $L''|K$ galoisch; cf. Beispiel 10.(1) und Aufgabe 17.(1).

Es ist $E'|K$ Kompositum von $E'|K$ und $E''|K$, via der Einbettungen. Da

$$[E' : K] \;=\; 6 \;\neq\; 6 \cdot 2 \;=\; [E' : K] \cdot [E'' : K] \; ,$$

sind $E'|K$ und $E''|K$ nicht linear disjunkt; cf. Lemma 44.

Ad (2). Die Aussage ist richtig.

Schreibe $L' = K(y')$ und $L'' = K(y'')$; cf. [**5,** Aufgabe 54]. Dann ist $L = K(y', y'')$. Sei E Zerfällungskörper von $\mu_{y',K}(X)\mu_{y'',K}(X) \in K[X]$. Es ist E Zerfällungskörper von $L|K$; cf. Beweis zu Lemma 11.(1). O.E. können wir diesen Zerfällungskörper E betrachten; cf. Lemma 11.(2).

Sei $\mu_{y',K}(X) = \prod_{i\in[1,n']}(X - y'_i) \in E[X]$, mit $y'_1 := y'$.

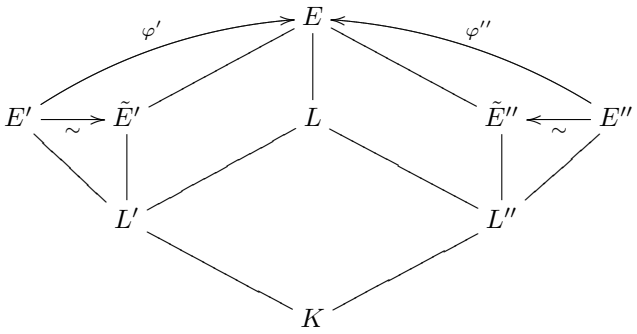
Sei $\mu_{y'',K}(X) = \prod_{i\in[1,n'']}(X - y''_i) \in E[X]$, mit $y''_1 := y''$.

Es ist $\tilde{E}' := K(\, y'_i \,:\, i \in [1,n']\,)$ Zerfällungskörper von $\mu_{y',K}(X) \in K[X]$ und also auch von $L'|K$; cf. Beweis zu Lemma 11.(2). Also gibt es einen Isomorphismus von E' nach $\tilde{E}'$, der auf L' identisch einschränkt; cf. Lemma 11.(2). Sei $\varphi' : E' \to E$ dessen Kompositum mit der Einbettung $\tilde{E}' \to E$.

Genauso ist $\tilde{E}'' := K(\, y''_j \,:\, j \in [1,n'']\,)$ Zerfällungskörper von $L''|K$. Also gibt es einen Isomorphismus von E'' nach $\tilde{E}''$, der auf L'' identisch einschränkt; cf. Lemma 11.(2). Sei $\varphi'' : E'' \to E$ dessen Kompositum mit der Einbettung $\tilde{E}'' \to E$.

Es ist $E|K$ Kompositum von $E'|K$ und $E''|K$ via φ' und φ'', da $\varphi'(E') = \tilde{E}' = K(\, y'_i \,:\, i \in [1,n']\,)$, da $\varphi''(E'') = \tilde{E}'' = K(\, y''_j \,:\, j \in [1,n'']\,)$ und da

$$E \;=\; K(\, y'_i\,,\, y''_j \,:\, i \in [1,n'],\, j \in [1,n'']\,)\;.$$



Ad (3). Die Aussage ist richtig.

Im Beweis zu (2) erhalten wir $L' = \tilde{E}'$ wegen $L'|K$ galoisch und $L'' = \tilde{E}''$ wegen $L''|K$ galoisch.

Der kleinste Teilkörper von E, der $L' = \tilde{E}'$ und $L'' = \tilde{E}''$ enthält, ist zugleich L und E. Also folgt $L = E$.

> Alternativ, es sind in (2) dann $y'_i \in L' = K(y')$ für $i \in [1,n']$ und $y''_i \in L'' = K(y'')$ für $i \in [1,n'']$. Also folgt
>
> $$E \;=\; K(\, y'_i\,,\, y''_j \,:\, i \in [1,n'],\, j \in [1,n'']\,) \;=\; K(y',y'') \;=\; L\;.$$

Ad (4). Die Aussage ist richtig.

Es ist $[L : K] \overset{1.}{=} [L : L'] \cdot [L' : K] \overset{2.}{=} [L : L''] \cdot [L'' : K]$. Da $[L' : K]$ und $[L'' : K]$ teilerfremd sind, ist $[L' : K]$ ein Teiler von $[L : L'']$.

Es ist $[L : L''] \cdot [L'' : K] = [L : K] \leqslant [L' : K] \cdot [L'' : K]$; cf. Bemerkung 42. Also ist $[L : L''] \leqslant [L' : K]$.

Zusammen folgt $[L : L''] = [L' : K]$, also $[L : K] = [L : L''] \cdot [L'' : K] = [L' : K] \cdot [L'' : K]$ und somit $L'|K$ und $L''|K$ linear disjunkt; cf. Lemma 44.

Ad (5). Die Aussage ist richtig.

Es ist $L|K$ galoisch; cf. (3). Sei $G := \mathrm{Gal}(L|K)$. Sei $N' := \mathrm{Gal}(L|L') \trianglelefteqslant G$. Es ist $\mathrm{Gal}(L'|K) = G/N'$. Sei $N'' := \mathrm{Gal}(L|L'') \trianglelefteqslant G$. Es ist $\mathrm{Gal}(L''|K) = G/N''$. Cf. **[5,** §3.5.2].

Da L Kompositum von L' und L'' ist, ist ein $\sigma \in G$, das in N' und N'' liegt, i.e. das L' und L'' elementweise fixiert, bereits die Identität. Denn der Teilkörper von L, der von σ elementweise fixiert wird, enthält L' und L'', ist also gleich L. Mit anderen Worten, es ist $N' \cap N'' = 1$. Es ist $N'N'' \trianglelefteqslant G$. Also ist die

Abbildung

$$\begin{array}{ccccc} N' & \times & N'' & \longrightarrow & N'N'' \\ (n' & , & n'') & \longmapsto & n'n'' \end{array}$$

nicht nur surjektiv, sondern auch injektiv. Denn ist $n'n'' = \tilde{n}'\tilde{n}''$ für $(n', n''), (\tilde{n}', \tilde{n}'') \in N' \times N''$, dann ist $\tilde{n}'^{-1}n' = \tilde{n}''n''^{-1}$ in $N' \cap N'' = 1$, und somit $\tilde{n}' = n'$ und $\tilde{n}'' = n''$.

Insbesondere ist $|N'| \cdot |N''| = |N' \times N''| = |N'N''|$.

Es sind $L'|K$ und $L''|K$ linear disjunkt genau dann, wenn $[L : K] = [L' : K] \cdot [L'' : K]$, i.e. wenn $|G| = |G/N'| \cdot |G/N''|$, i.e. wenn $|G| = |N'| \cdot |N''|$; cf. Lemma 44.

Die Elemente aus L, die von allen Elementen von N' und von N'' fixiert werden, sind die in $L' \cap L''$. Also ist $\mathrm{Gal}(L|L' \cap L'') = N'N''$.

Somit ist genau dann $L' \cap L'' = K$, wenn $N'N'' = G$, i.e. wenn $|N'N''| = |G|$, i.e. wenn $|N'| \cdot |N''| = |G|$, i.e. wenn $L'|K$ und $L''|K$ linear disjunkt sind.

Ad (6). Die Aussage ist falsch.

Sei $K := \mathbf{Q}$. Sei $L := \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$. Sei $L' := \mathbf{Q}(\sqrt[3]{2})$. Sei $L'' := \mathbf{Q}(\zeta_3\sqrt[3]{2})$. Es sind $L'|K$ und $L''|K$ nicht linear disjunkt; cf. Beispiel 45.(3). Es ist $L' \neq L''$, da $L' \subseteq \mathbf{R}$, aber $\zeta_3\sqrt[3]{2} \notin \mathbf{R}$. Somit ist $[L' \cap L'' : K]$ ein echter Teiler von $[L' : K] = 3$, also gleich 1. Es folgt $L' \cap L'' = K$.

Aufgabe 24

Ad (1).

Gelte (i). Sei $\emptyset \subset M \subseteq \mathrm{Ideale}(R)$. *Annahme,* es hat M kein maximales Element. Sei $\mathfrak{a}_1 \in M$ gewählt, möglich, da $M \neq \emptyset$. Da M kein maximales Element enthält, gibt es ein $\mathfrak{a}_2 \in M$ mit $\mathfrak{a}_1 \subset \mathfrak{a}_2$. Da M kein maximales Element enthält, gibt es ein $\mathfrak{a}_3 \in M$ mit $\mathfrak{a}_2 \subset \mathfrak{a}_3$. Usf. Wir erhalten eine Kette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$$

Sei $\mathfrak{a} := \bigcup_{i \geqslant 1} \mathfrak{a}_i$. Es ist $\mathfrak{a}$ ein Ideal in R, da $0 \in \mathfrak{a}$ und da für $r, r' \in R$ und $a, a' \in \mathfrak{a}$ es ein $j \geqslant 1$ gibt mit $a, a' \in \mathfrak{a}_j$, sodaß $ra + r'a' \in \mathfrak{a}_j \subseteq \mathfrak{a}$ folgt. Schreibe $\mathfrak{a} = (\, x_i : i \in [1, n]\,)$ mit $n \geqslant 0$ und $x_i \in R$ geeignet. Es gibt ein $k \geqslant 1$ mit $x_i \in \mathfrak{a}_k$ für $i \in [1, n]$. Also wird

$$\mathfrak{a}_k \subset \mathfrak{a}_{k+1} \subseteq \mathfrak{a} = (\, x_i : i \in [1, n]\,) \subseteq \mathfrak{a}_k\,,$$

und wir haben einen *Widerspruch.*

Gelte (ii). Sei $\mathfrak{a} \subseteq R$ ein Ideal. *Annahme,* es ist $\mathfrak{a}$ nicht endlich erzeugt. Wähle $a_1 \in \mathfrak{a}$. Da $\mathfrak{a}$ nicht endlich erzeugt ist, ist $\mathfrak{a}_1 := (\, a_1\,) \subset \mathfrak{a}$. Wähle $a_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1$. Da $\mathfrak{a}$ nicht endlich erzeugt ist, ist $\mathfrak{a}_2 := (\, a_1\,, a_2\,) \subset \mathfrak{a}$. Wähle $a_3 \in \mathfrak{a} \smallsetminus \mathfrak{a}_2$. Da $\mathfrak{a}$ nicht endlich erzeugt ist, ist $\mathfrak{a}_3 := (\, a_1\,, a_2\,, a_3\,) \subset \mathfrak{a}$. Usf.

Sei $M := \{\, \mathfrak{a}_i : i \in \mathbf{Z}_{\geqslant 1}\,\}$. Es hat M ein maximales Element. Mithin gibt es ein $k \geqslant 1$ mit $\mathfrak{a}_k \not\subset \mathfrak{a}_i$ für alle $i \geqslant 1$. Aber $\mathfrak{a}_k \subset \mathfrak{a}_{k+1}$, und wir haben einen *Widerspruch.*

Cf. auch Aufgabe 2.(1).

Ad (2).

Sei R noethersch. Wir haben zu zeigen, daß $R[X]$ noethersch ist.

Wir haben die Abbildung

$$\begin{array}{ccc} R[X]^\times & \xrightarrow{\ \ell\ } & R^\times \\ f(X) & \longmapsto & a_{\deg(f)}\,, \end{array}$$

wobei $f(X) = \sum_{i \in [0, \deg(f)]} a_i X^i$.

Wir haben für $n \geqslant 0$ die Abbildung

$$\begin{array}{rcl} \text{Ideale}(R[X]) & \xrightarrow{\ell_n} & \text{Ideale}(R) \\ \mathfrak{b} & \longmapsto & \ell(\{\, f(X) \in \mathfrak{b} \,:\, \deg(f(X)) = n \,\}) \cup \{0\} \,, \end{array}$$

denn für $r, \tilde{r} \in R^\times$ und $f(X), \tilde{f}(X) \in R[X]$ mit $\deg(f) = \deg(\tilde{f}) = n$ ist $r\ell(f(X)) + \tilde{r}\ell(\tilde{f}(X)) = \ell(rf(X) + \tilde{r}\tilde{f}(X))$, falls $r\ell(f(X)) + \tilde{r}\ell(\tilde{f}(X)) \neq 0$.

Sei nun $\mathfrak{b} \in \text{Ideale}(R[X])$. Wir haben zu zeigen, daß $\mathfrak{b}$ endlich erzeugt ist.

Für $n \geqslant 0$ ist $\ell_n(\mathfrak{b}) \subseteq \ell_{n+1}(\mathfrak{b})$, da wenn $f(X) \in R[X]$ mit $\deg(f(X)) = n$ vorliegt und also $\ell(f(X)) \in \ell_n(\mathfrak{b})$ liegt, dann $\deg(Xf(X)) = n+1$ ist und folglich auch $\ell(f(X)) = \ell(Xf(X)) \in \ell_{n+1}(\mathfrak{b})$ liegt. Da R noethersch ist, hat die Menge $\{\, \ell_n(\mathfrak{b}) \,:\, n \geqslant 0 \,\}$ ein maximales Element $\ell_k(\mathfrak{b})$ für ein $k \geqslant 0$. Da $\ell_k(\mathfrak{b}) \subseteq \ell_n(\mathfrak{b})$ für $n \in \mathbf{Z}_{\geqslant k}$, ist also $\ell_k(\mathfrak{b}) = \ell_n(\mathfrak{b})$ für $n \in \mathbf{Z}_{\geqslant k}$.

Für $n \in [0,k]$ schreiben wir nun

$$\ell_n(\mathfrak{b}) \;=\; (\, \ell(f_{n,i}(X)) \,:\, i \in [1, s_n] \,)$$

für ein geeignetes $s_n \geqslant 0$ und geeignete $f_{n,i}(X) \in \mathfrak{b}$ mit $\deg(f_{n,i}(X)) = n$. Wir *behaupten*

$$\mathfrak{b} \;\overset{!}{=}\; (\, f_{n,i}(X) \,:\, n \in [0,k],\; i \in [1, s_n] \,) =: \mathfrak{c} \,.$$

Zu zeigen ist nur $\mathfrak{b} \overset{!}{\subseteq} \mathfrak{c}$.

Sei $g(X) \in \mathfrak{b}$ gegeben. Wir müssen $g(X) \overset{!}{\in} \mathfrak{c}$ zeigen. O.E. ist $g(X) \neq 0$.

Wir führen eine Induktion über $d := \deg(g)$.

Ist $d = 0$, so ist $g(X) = \ell(g(X)) \in \ell_0(\mathfrak{b}) = (\, \ell(f_{0,i}(X)) \,:\, i \in [1, s_0] \,) = (\, f_{0,i}(X) \,:\, i \in [1, s_0] \,) \subseteq \mathfrak{c}$.

Sei nun $d \geqslant 1$. Sei $m := \min\{k, d\} \in [0,k]$. Es ist $\ell(g(X)) \in \ell_d(\mathfrak{b}) = \ell_m(\mathfrak{b})$. Somit finden wir $r_i \in R$ für $i \in [1, s_m]$ mit

$$\ell(g(X)) \;=\; \sum_{i \in [1, s_m]} r_i \ell(f_{m,i}(X)) \,.$$

Schreibe $\tilde{g}(X) := g(X) - \sum_{i \in [1,s_m]} r_i f_{m,i}(X) \in \mathfrak{b}$. Es ist $\tilde{g}(X) = 0$ oder $\deg(\tilde{g}) < \deg(g)$. Mit Induktion ist $\tilde{g}(X) \in \mathfrak{c}$. Also ist auch

$$g(X) \;=\; \underbrace{\tilde{g}(X)}_{\in \mathfrak{c}} + \underbrace{\sum_{i \in [1,s_m]} r_i f_{m,i}(X))}_{\in \mathfrak{c}} \;\in\; \mathfrak{c} \,.$$

Diese Aussage heißt Hilbertscher Basissatz.

Ad (3). Schreibe die Restklassenabbildung $\rho : R \to R/\mathfrak{a}$, $r \mapsto r + \mathfrak{a}$.

Sei $\mathfrak{b} \in \text{Ideale}(R/\mathfrak{a})$. Es ist $\rho^{-1}(\mathfrak{b}) \in \text{Ideale}(R)$, denn für $r, r' \in R$ und $a, a' \in \rho^{-1}(\mathfrak{b})$ ist $\rho(a), \rho(a') \in \mathfrak{b}$ und folglich $\rho(ra + r'a') = r\rho(a) + r'\rho(a') \in \mathfrak{b}$, i.e. $ra + r'a' \in \rho^{-1}(\mathfrak{b})$.

Da R noethersch ist, schreiben wir $\rho^{-1}(\mathfrak{b}) = (\, x_i \,:\, i \in [1,n] \,)$ mit $n \geqslant 0$ und $x_i \in R$ geeignet. Es wird

$$\mathfrak{b} \;=\; \rho(\rho^{-1}(\mathfrak{b})) \;=\; (\, \rho(x_i) \,:\, i \in [1,n] \,) \,,$$

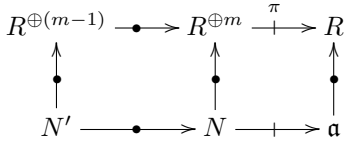
denn für $\sum_{i \in [1,n]} r_i x_i$ mit $r_i \in R$ wird $\rho(\sum_{i \in [1,n]} r_i x_i) = \sum_{i \in [1,n]} r_i \rho(x_i)$.

Ad (4).

Zum Beweis wiederholen wir Argumente zur Lösung von Aufgabe 13.(2), entsprechend abgeändert. Damals kannten wir nur Hauptidealbereiche, die allgemeinere Situation über einem noetherschen kommutativen Ring konnten wir da noch nicht behandeln.

Wir führen eine Induktion über $m \geqslant 0$. Für $m = 0$ ist die Aussage richtig. Sei nun $m \geqslant 1$.

Betrachte das folgende Diagramm von R-Moduln und R-linearen Abbildungen.



Hierbei ist π die Projektion auf den letzten Tupeleintrag. Die horizontalen Abbildungen links sind Inklusionen von Kernen. Die vertikalen Abbildungen sind Inklusionen. Das Kompositum $N \to R$ hat als Bild einen Teilmodul von R, i.e. ein Ideal $\mathfrak{a}$ in R, welches wegen R noethersch endlich erzeugt ist, sagen wir $\mathfrak{a} = (\, a_1 \,, \ldots \,, a_\ell \,)$ für ein $\ell \geqslant 0$ und geeignete Elemente $a_i \in \mathfrak{a}$ für $i \in [1, \ell]$.

Es ist N' der Kern der Abbildung $N \to \mathfrak{a}$. Nach Induktion können wir $N' = {}_R\langle\, n'_1 \,, \ldots \,, n'_k \,\rangle$ schreiben für ein $k \geqslant 0$ und geeignete Elemente $n'_i \in N'$ für $i \in [1, k]$.

Wähle $n_i \in N$ mit $\pi(n_i) = a_i$ für $i \in [1, \ell]$. Wir wollen

$$N \overset{!}{=} {}_R\langle\, n'_1 \,, \ldots \,, n'_k \,, n_1 \,, \ldots \,, n_\ell \,\rangle$$

zeigen. Zu zeigen ist $\overset{!}{\subseteq}$. Sei $n \in N$ gegeben. Schreibe $\pi(n) = \sum_{i \in [1,\ell]} r''_i a_i$ mit geeigneten $r''_i \in R$ für $i \in [1, \ell]$. Dann ist

$$\pi(n - \textstyle\sum_{i \in [1,\ell]} r''_i n_i) \;=\; \pi(n) - \sum_{i \in [1,\ell]} r''_i a_i \;=\; 0 \,,$$

also $n - \sum_{i \in [1,\ell]} r''_i n_i \in N'$, und wir können

$$n - \textstyle\sum_{i \in [1,\ell]} r''_i n_i \;=\; \sum_{j \in [1,k]} r'_j n'_j$$

schreiben mit geeigneten $r'_j \in R$ für $j \in [1, k]$. Somit liegt in der Tat

$$n \;=\; (\textstyle\sum_{j \in [1,k]} r'_j n'_j) + (\sum_{i \in [1,\ell]} r''_i n_i) \;\in\; {}_R\langle\, n'_1 \,, \ldots \,, n'_k \,, n_1 \,, \ldots \,, n_\ell \,\rangle \,.$$

Ad (5). Es enthält B eine K-lineare Basis $\underline{y}$ von L; cf. Lemma 28. Sei $X := {}_A\langle \underline{y} \rangle$. Es ist

$$X \;\subseteq\; B \;\subseteq\; B^\# \;\subseteq\; X^\# \,;$$

cf. Bemerkung 30, Lemma 31.(2). Es ist $X^\# = {}_A\langle \underline{y'} \rangle$, wobei $\underline{y'}$ die zu $\underline{y}$ bezüglich Spurbilinearform duale Basis ist; cf. Lemma 31. Insbesondere ist $X^\#$ ein endlich erzeugter freier A-Modul.

Sei $\mathfrak{b} \subseteq B$ ein Ideal. Wir haben zu zeigen, daß $\mathfrak{b}$ ein endlich erzeugtes Ideal ist, i.e. ein endlich erzeugter B-Teilmodul von B.

Es genügt zu zeigen, daß $\mathfrak{b}$ ein endlich erzeugter A-Teilmodul von B ist, da ein A-Erzeugendensystem a fortiori auch ein B-Erzeugendensystem ist. Nach isomorpher Ersetzung von $X^\#$ durch eine direkte Summe von Kopien von A folgt dies mit (4).

Speziell folgt für $\mathfrak{b} = B$, daß B ein endlich erzeugter A-Modul ist.

Ad (6). Schreibe $R := \prod_{k \in \mathbf{Z}_{\geqslant 1}} \mathbf{C}$. Schreibe für $s \geqslant 0$

$$\mathfrak{a}_s \;:=\; \{\, (z_k)_k \in R \,:\, z_k = 0 \text{ für } k \geqslant s+1 \,\} \;\in\; \text{Ideale}(R) \,.$$

Es ist $\mathfrak{a}_s \subset \mathfrak{a}_{s+1}$ für $s \geqslant 0$. Also hat $\{\, \mathfrak{a}_s \,:\, s \geqslant 0 \,\}$ kein maximales Element. Mithin ist R nicht noethersch.

Ad (7). Es ist $\mathbf{C}$ als Körper ein noetherscher kommutativer Ring. Mit (2) folgt $\mathbf{C}[X]$ noethersch. Mit (2) folgt $\mathbf{C}[X][Y] = \mathbf{C}[X,Y]$ noethersch.

Sei

$$R \;:=\; \mathbf{C}[\, XY^k \,:\, k \geqslant 0\,] \;\subseteq\; \mathbf{C}[X,Y]\,.$$

Sei darin das Ideal

$$\mathfrak{a} \;:=\; (\, XY^k \,:\, k \geqslant 0\,) \;\subseteq\; R$$

betrachtet. Um zu zeigen, daß es nicht endlich erzeugt ist, genügt es zu zeigen, daß für $\ell \geqslant 0$ und

$$\mathfrak{a}_\ell \;:=\; (\, XY^k \,:\, k \in [0,\ell]\,)$$

stets $\mathfrak{a}_\ell \subset \mathfrak{a}_{\ell+1}$ ist. Denn es ist $\mathfrak{a} = \bigcup_{\ell \geqslant 0} \mathfrak{a}_\ell$. *Hätte* also $\mathfrak{a}$ endlich viele Erzeuger, dann wären diese bereits in $\mathfrak{a}_m$ für ein $m \geqslant 0$ enthalten, was wegen $\mathfrak{a} \subseteq \mathfrak{a}_m \subset \mathfrak{a}_{m+1} \subseteq \mathfrak{a}$ *nicht* geht.

Es genügt also, $XY^{\ell+1} \overset{!}{\notin} \mathfrak{a}_\ell$ nachzuweisen. Aber jedes Element von $\mathfrak{a}_\ell$ ist $\mathbf{C}$-Linearkombination von Monomen, die Grad 1 in X und dabei Grad $\in [0,\ell]$ in Y haben, oder aber Grad $\geqslant 2$ in X haben. Denn in R stehen als Monome nur 1 oder aber Monome mit Grad $\geqslant 1$ in X zur Verfügung.

Anmerkung. *Für einen kommutativen Ring A folgt aus $A_\mathfrak{p}$ noethersch für alle $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ nicht unbedingt A noethersch.*

Zunächst müssen wir dazu die Definition den allgemeineren Gegebenheiten anpassen. Es besteht $A_\mathfrak{p}$ aus Brüchen $\frac{a}{s}$ mit $a \in A$, $s \in A \smallsetminus \mathfrak{p}$. Hierbei ist ein solcher Bruch eine Äquivalenzklasse von Paaren (a,s) mit $a \in A$, $s \in A \smallsetminus \mathfrak{p}$, mit der Äquivalenzrelation erzeugt von $((a,s),(at,st))$, wobei $t \in A \smallsetminus \mathfrak{p}$. Addition und Multiplikation folgen den Regeln der Bruchrechnung.

Sei K ein Körper. Sei I eine unendliche Menge. Sei $K^I := \{\, (x_i)_{i\in I} \,:\, x_i \in K\,\}$. Schreibe kurz $x = (x_i)_i := (x_i)_{i\in I}$. Mit eintragsweiser Addition und Multiplikation wird K^I ein kommutativer Ring.

Schreibe $e_k := (\partial_{k,i})_i \in K^I$ für $k \in I$. Für eine endliche Teilmenge M von I sei $e_M := \sum_{k\in M} e_k$.

Schreibe $\mathfrak{u} := K^{\oplus I}$. Dies ist ein Ideal in K^I.

Für $M \subseteq I$ sei $K^{\oplus M} := \{\, x \in K^{\oplus I} \,:\, x_i = 0 \text{ für } i \in I \smallsetminus M\,\}$.

Sei $A := K\cdot 1 \oplus \mathfrak{u} \subseteq K^I$. Dies ist ein Teilring in K^I.

Es ist A nicht noethersch. Denn ist $\mathbf{Z}_{\geqslant 1} \to I$, $k \mapsto i_k$ eine injektive Abbildung, dann ist

$$K^{\oplus\{i_1\}} \;\subset\; K^{\oplus\{i_1\,,\,i_2\}} \;\subset\; K^{\oplus\{i_1\,,\,i_2\,,\,i_3\}} \;\subset\; \ldots$$

eine nichtabbrechende echt aufsteigende Kette von Idealen von A; cf. Definition 50.

Sei ein Primideal $\mathfrak{p}$ in A gegeben.

Fall: es gibt kein $j \in I$ mit $e_j \notin \mathfrak{p}$. Dann ist $\mathfrak{u} \subseteq \mathfrak{p}$. Da $A/\mathfrak{u} \simeq K$, folgt $\mathfrak{u}$ maximal und also $\mathfrak{p} = \mathfrak{u}$.

Sei $\frac{\lambda\cdot 1+u}{\mu\cdot 1+v} \in A_\mathfrak{p}$ gegeben, mit $u,\, v \in \mathfrak{u}$, mit $\lambda \in K$ und mit $\mu \in K^\times$. Sei $M := \{\, i \in I \,:\, u_i \neq 0 \text{ oder } v_i \neq 0\,\}$. Dann ist $ue_M = u$ und $ve_M = v$. Ferner ist $1 - e_M \in A \smallsetminus \mathfrak{p}$. Folglich ist

$$\frac{\lambda\cdot 1+u}{\mu\cdot 1+v} \;=\; \frac{(\lambda\cdot 1+u)(1-e_M)}{(\mu\cdot 1+v)(1-e_M)} \;=\; \frac{\lambda(1-e_M)}{\mu(1-e_M)} = \frac{\lambda}{\mu}\,.$$

Hieraus folgt $K \xrightarrow{\sim} A_\mathfrak{p}$ als Ringe. Insbesondere ist $A_\mathfrak{p}$ noethersch.

Fall: es gibt ein $j \in I$ mit $e_j \notin \mathfrak{p}$. Schreibe $I' := I \smallsetminus \{j\}$. Schreibe $\mathfrak{u}' := K^{\oplus I'}$.

Ist $i \in I'$, dann ist $e_i \in \mathfrak{p}$. Denn sonst *wären* $e_i\,,\, e_j \notin \mathfrak{p}$, aber $e_ie_j = 0 \in \mathfrak{p}$, im *Widerspruch* zu $\mathfrak{p}$ prim. Folglich ist $\mathfrak{u}' \subseteq \mathfrak{p}$.

Es ist $A/\mathfrak{u}' = {}_K\langle 1+\mathfrak{u}', e_j+\mathfrak{u}'\rangle$. Wir haben einen Isomorphismus

$$\begin{array}{rcl} K[X]/(X^2-X) & \xrightarrow{\sim} & A/\mathfrak{u}' \\ X+(X^2-X) & \mapsto & e_j+\mathfrak{u}'\,. \end{array}$$

Da $K[X]/(X^2-X) = K[X]/(X(X-1))$ genau die beiden Primideale $(X)/(X^2-X)$ und $(X-1)/(X^2-X)$ hat, hat A genau die beiden Primideale $(e_j-1)+\mathfrak{u}' = (e_j-1)$ und $(e_j)+\mathfrak{u}' = \mathfrak{u}$, die $\mathfrak{u}'$ enthalten. Da $e_j \notin \mathfrak{p}$ liegt, folgt $\mathfrak{p} = (e_j-1) = \mathfrak{u}' \oplus {}_K\langle 1-e_j\rangle$.

Sei $\frac{\lambda\cdot 1+u}{\mu\cdot 1+v} \in A_{\mathfrak{p}}$ gegeben, mit $u, v \in \mathfrak{u}$, mit $\lambda, \mu \in K$, wobei $v_j + \mu \neq 0$ ist. Es ist $e_j \in A \smallsetminus \mathfrak{p}$. Also folgt

$$\frac{\lambda \cdot 1 + u}{\mu \cdot 1 + v} \;=\; \frac{(\lambda \cdot 1 + u)e_j}{(\mu \cdot 1 + v)e_j} \;=\; \frac{(\lambda + u_j)e_j}{(\mu + v_j)e_j} \;=\; \frac{\lambda + u_j}{\mu + v_j}\,.$$

Hieraus folgt $K \xrightarrow{\sim} A_{\mathfrak{p}}$ als Ringe. Insbesondere ist $A_{\mathfrak{p}}$ noethersch.

Gibt es auch einen Integritätsbereich A, den man als Gegenbeispiel anführen kann?

Aufgabe 25

Ad (1). Sei $E|K$ ein Zerfällungskörper von $f(X) \in K[X]$; cf. **[5,** §2.5.2]. Sei $n := \deg(f)$. Schreibe $f(X) = \prod_{i\in[1,n]}(X - u_i)$ mit $u_i \in E$ für $i \in [1, n]$. Da $E[X]$ ein Hauptidealbereich ist, gilt darin die bis auf Reihenfolge eindeutige Zerlegung in irreduzible Faktoren; cf. **[5,** §1.7.4], Aufgabe 2.(2, 3). Sei $k := \deg(g)$. Somit ist o.E. $g(X) = \prod_{i\in[1,k]}(X - u_i)$.

Nun ist $u_i \in \Gamma_E(A)$ als Nullstelle von $f(X)$ in E für $i \in [1, n]$. Also ist $g(X) \in \Gamma_E(A)[X] \cap K[X] = \Gamma_K(A)[X] = A[X]$, letzteres, da A ganzabgeschlossen ist.

Ad (2). Ist $\mu_{y,K}(X) \in A[X]$, dann ist y als Nullstelle von $\mu_{y,K}(X)$ in B.

Ist umgekehrt $y \in B$, dann gibt es ein $f(X) \in A[X]$ normiert mit $f(y) = 0$. Also ist $\mu_{y,K}(X)$ ein Teiler von $f(X)$ in $K[X]$. Gemäß (1) folgt $\mu_{y,K}(X) \in A[X]$.

Cf. Aufgabe 2.(8).

Aufgabe 26

Ad (1). O.E. ist $n \geqslant 2$.

Es genügt zu zeigen, daß $(\partial_{j,i})_i$ im Bild von χ liegt für alle $j \in [1, n]$.

Es genügt dazu zu zeigen, daß für vorgegebene $j, k \in [1, n]$ ein Element $(x_i)_i$ mit $x_j = 1$ und $x_k = 0$ im Bild von χ liegt. Denn das Produkt solcher Elemente, für ein gegebenes $j \in [1, n]$ genommen über $k \in [1, n]$, ist dann von der gewünschten Form.

Es ist $\mathfrak{a}_j + \mathfrak{a}_k = R$. Also können wir $a_j \in \mathfrak{a}_j$ und $a_k \in \mathfrak{a}_k$ mit $a_j + a_k = 1$ wählen. Nun hat $\chi(a_k) = (a_k + \mathfrak{a}_i)_i$ die Einträge $a_k + \mathfrak{a}_j = 1 - a_j + \mathfrak{a}_j = 1 + \mathfrak{a}_j = 1$ an Position j und $a_k + \mathfrak{a}_k = 0 + \mathfrak{a}_k = 0$ an Position k.

Die Aussage heißt auch Chinesischer Restsatz.

Ad (2). Dank (1) bleibt uns $\mathfrak{p}^k + \mathfrak{q}^\ell \stackrel{!}{=} D$ zu zeigen für $\mathfrak{p}, \mathfrak{q} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D)$ mit $\mathfrak{p} \neq \mathfrak{q}$ und für $k, \ell \geqslant 1$.

Es ist $\mathfrak{p}^k + \mathfrak{q}^\ell \in \mathrm{Ideale}(D)$. Da jedes Ideal ungleich (1) von D in einem maximalen Ideal liegt, genügt es zu zeigen, daß $\mathfrak{p}^k + \mathfrak{q}^\ell$ in keinem maximalen Ideal liegt; cf. Bemerkung 51.(4).

Dafür genügt es zu zeigen, daß $\mathfrak{p}^k$ in keinem anderen maximalen Ideal als $\mathfrak{p}$ liegt. Denn genauso liegt dann $\mathfrak{q}^\ell$ in keinem anderen maximalen Ideal als $\mathfrak{q}$. Läge das Ideal $\mathfrak{p}^k + \mathfrak{q}^\ell$, das $\mathfrak{p}^k$ und $\mathfrak{q}^\ell$ enthält, in einem maximalen Ideal, so müßte dies demnach sowohl gleich $\mathfrak{p}$ als auch gleich $\mathfrak{q}$ sein, was nicht geht.

Annahme, es ist $\mathfrak{p}^k \subseteq \mathfrak{r}$ mit $\mathfrak{r} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(D) \smallsetminus \{\mathfrak{p}\}$. Dann ist $\mathfrak{p}^k\mathfrak{r}^{-1} \subseteq D$. Es ist $\mathrm{v}_{\mathfrak{r}}(\mathfrak{p}^k\mathfrak{r}^{-1}) = -1 < 0$ gemäß Lemma 65. Dies steht im *Widerspruch* zu Bemerkung 66.(1), wonach Ideale in D überall Bewertung $\geqslant 0$ haben.

Aufgabe 27

Schreibe $\alpha := \sqrt{-5}$. Es ist $\mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Es ist $\mathrm{Gal}(\mathbf{Q}(\alpha)|\mathbf{Q}) = \{\mathrm{id}, \sigma\}$, wobei $\sigma(\alpha) = -\alpha$ ist.

Ad (1). Sei $\mathfrak{a} := (2, 1+\alpha)$. Es ist $\mathfrak{a}^2 = (2, 2+2\alpha, (1+\alpha)^2) = (2, 2+2\alpha, -4+2\alpha) = (2)$.

Wir haben zu zeigen, daß $\mathfrak{a}$ kein Hauptideal ist.

Ist $\mathfrak{a} = (x)$ für ein $x \in \mathbf{Z}[\alpha]$, dann ist $|R/(x)|$ die Determinante der $\mathbf{Z}$-linearen Multiplikationsabbildung $\lambda_x : R \to R$, $y \mapsto xy$; cf. Aufgabe 14.(2). I.e. es ist $|R/(x)| = |\,\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(x)|$; cf. Definition 12.

Nun ist für $a + b\alpha \in \mathbf{Z}[\alpha]$ mit $a, b \in \mathbf{Z}$ bekanntlich $|\,\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(a+b\alpha)| = a^2 + 5b^2$. Es genügt also zu zeigen, daß $|\mathbf{Z}[\alpha]/\mathfrak{a}|$ nicht von dieser Form ist.

Es ist

$$\mathfrak{a} \;=\; (2, 1+\alpha) \;=\; {}_{\mathbf{Z}}\langle 2, 2\alpha, 1+\alpha, (1+\alpha)\alpha\rangle \;=\; {}_{\mathbf{Z}}\langle 2, 2\alpha, 1+\alpha, -5+\alpha\rangle \;=\; {}_{\mathbf{Z}}\langle 2, 1+\alpha\rangle\ .$$

Also ist $|\mathbf{Z}[\alpha]/\mathfrak{a}| = |\det \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)| = 2$; cf. Aufgabe 14.(2). Es sind nun in der Tat

$$-2,\ 2 \;\notin\; \{\, a^2 + 5b^2 \,:\, a, b \in \mathbf{Z} \,\} \;=\; \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathbf{Z}[\alpha])\ .$$

Folglich ist $\mathfrak{a}$ kein Hauptideal.

Ad (2). Es ist

$$(3, 1+2\alpha)(3, 1-2\alpha) \;=\; (9, 3+6\alpha, 3-6\alpha, 21) \;=\; (3)$$

und

$$(7, 4+\alpha)(7, 4-\alpha) \;=\; (49, 28+7\alpha, 28-7\alpha, 21) \;=\; (7)\ .$$

Es ist $(3, 1+2\alpha) = {}_{\mathbf{Z}}\langle 3, 3\alpha, 1+2\alpha, -10+\alpha\rangle = {}_{\mathbf{Z}}\langle 1-\alpha, 3\alpha\rangle$. Hierfür kann man mit $A = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \\ 1 & 2 \\ -10 & 1 \end{smallmatrix}\right)$ Matrizen $S \in \mathrm{GL}_4(\mathbf{Z})$ und $T \in \mathrm{GL}_2(\mathbf{Z})$ so suchen, daß $D := SAT$ diagonal ist und dann die Koeffizienten der Basis den Zeilen von $SA = DT^{-1}$ entnehmen. Inbesondere ist $|\mathbf{Z}[\alpha]/(3, 1+2\alpha)| = |\det \left(\begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix}\right)| = 3$, mithin $\mathbf{Z}/(3) \to \mathbf{Z}[\alpha]/(3, 1+2\alpha)$, $z + (3) \mapsto z + (3, 1+2\alpha)$ ein Isomorphismus und also $(3, 1+2\alpha)$ ein Primideal.

Da $(3, 1+2\alpha)$ ein Primideal ist, trifft dies auch auf $\sigma((3, 1+2\alpha)) = (3, 1-2\alpha)$ zu, denn $\sigma|^{\mathbf{Z}[\alpha]}_{\mathbf{Z}[\alpha]}$ ist ein Ringautomorphismus von $\mathbf{Z}[\alpha]$.

Es ist $(7, 4+\alpha) = {}_{\mathbf{Z}}\langle 7, 7\alpha, 4+\alpha, -5+4\alpha\rangle = {}_{\mathbf{Z}}\langle 1+2\alpha, 7\alpha\rangle$. Inbesondere ist $|\mathbf{Z}[\alpha]/(7, 4+\alpha)| = |\det \left(\begin{smallmatrix} 1 & 2 \\ 0 & 7 \end{smallmatrix}\right)| = 7$, mithin $\mathbf{Z}/(7) \to \mathbf{Z}[\alpha]/(7, 4+\alpha)$, $z + (7) \mapsto z + (7, 4+\alpha)$ ein Isomorphismus und also $(7, 4+\alpha)$ ein Primideal.

Da $(7, 4+\alpha)$ ein Primideal ist, trifft dies auch auf $\sigma((7, 4+\alpha)) = (7, 4-\alpha)$ zu.

Somit wird

$$(21) \;=\; (3)\cdot(7) \;=\; (3, 1+2\alpha)(3, 1-2\alpha)(7, 4+\alpha)(7, 4-\alpha)$$

die Zerlegung von (21) in Primideale.

Es ist

$$(21) \;=\; (3)\cdot(7) \;=\; (1+2\alpha)(1-2\alpha) \;=\; (4+\alpha)(4-\alpha)\ .$$

Da $3,\ 7 \notin \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathbf{Z}[\alpha])$ liegen und da $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(7) = 49$, $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(3) = 9$, $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(1 \pm 2\alpha) = 21$ und $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(4 \pm \alpha) = 21$ ist, sind alle angeführten Idealerzeuger irreduzibel.

Daß es sich um drei wesentlich verschiedene Faktorisierungen handelt, die nicht durch Faktorenvertauschung und Multiplikation der Erzeuger mit Einheiten auseinander hervorgehen, wird sich aus der Verfeinerung in Produkte von Primidealen ergeben.

Es ist, wie oben schon bemerkt,

$$\begin{aligned} (3) &= (3, 1+2\alpha)(3, 1-2\alpha) \\ (7) &= (7, 4+\alpha)(7, 4-\alpha)\ . \end{aligned}$$

Also können wir verfeinern zu

$$(21) \;=\; (3)\cdot(7) \;=\; ((3,1+2\alpha)(3,1-2\alpha))\cdot((7,4+\alpha)(7,4-\alpha))\;.$$

Unter Beachtung von $(1+2\alpha)(1-2\alpha)=21$ wird

$$\begin{aligned}(3,1+2\alpha)(7,4+\alpha) &= (21,12+3\alpha,7(1+2\alpha),(1+2\alpha)(4+\alpha))\\ &= (21,(1+2\alpha)(2-\alpha),7(1+2\alpha),(1+2\alpha)(4+\alpha))\\ &= (1+2\alpha)\;.\end{aligned}$$

Anwendung von σ gibt hieraus

$$(3,1-2\alpha)(7,4-\alpha) \;=\; (1-2\alpha)\;.$$

Also können wir verfeinern zu

$$(21) \;=\; (1+2\alpha)\cdot(1-2\alpha) \;=\; ((3,1+2\alpha)(7,4+\alpha))\cdot((3,1-2\alpha)(7,4-\alpha))\;.$$

Unter Beachtung von $(4-\alpha)(4+\alpha)=21$ wird

$$\begin{aligned}(3,1+2\alpha)(7,4-\alpha) &= (21,3(4-\alpha),7+14\alpha,(1+2\alpha)(4-\alpha))\\ &= (21,3(4-\alpha),(4-\alpha)(-2+3\alpha),(1+2\alpha)(4-\alpha))\\ &= (4-\alpha)\;.\end{aligned}$$

Anwendung von σ gibt hieraus

$$(3,1-2\alpha)(7,4+\alpha) \;=\; (4+\alpha)\;.$$

Also können wir verfeinern zu

$$(21) \;=\; (4+\alpha)\cdot(4-\alpha) \;=\; ((3,1-2\alpha)(7,4+\alpha))\cdot((3,1+2\alpha)(7,4-\alpha))\;.$$

Dieses Phänomen der "unterschiedlichen Klammerungen" einer Primidealfaktorzerlegung kann als Erklärung für die nicht mehr eindeutigen Faktorisierungen in von irreduziblen Elementen erzeugte Ideale dienen.

Ad (3.i). Sei $K=\mathbf{Q}(\alpha)$. Sei $p=2$. Sei, wie in (1), $\mathfrak{a}:=(2,1+\alpha)$. Es ist $\mathfrak{a}^2=(2)$. Das allein zeigt schon, daß in der Primidealfaktorzerlegung von (2) alle Exponenten der auftretenden Primidealfaktoren durch 2 teilbar sind. Und es muß mindestens ein solcher Faktor auftreten, da $(2)\neq(1)$.

Genauer, es ist $\mathbf{Z}/(2)\to\mathbf{Z}[\alpha]/\mathfrak{a}$, $z+(2)\mapsto z+\mathfrak{a}$ als Ringmorphismus von einem Körper zu einem Ring ungleich 0 eine injektive Abbildung. Da, wie in (1) festgestellt, $|\mathbf{Z}[\alpha]/\mathfrak{a}|=2$ ist, ist dieser Ringmorphismus ein Isomorphismus. Insbesondere ist auch $\mathbf{Z}[\alpha]/\mathfrak{a}$ ein Körper, also $\mathfrak{a}\subset\mathbf{Z}[\alpha]$ ein maximales Ideal, also ein Primideal.

Ad (3.ii). Sei $K=\mathbf{Q}(\mathrm{i})$. Es ist $\mathcal{O}_{\mathbf{Q}(\mathrm{i})}=\mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Sei $p=2$. Es ist $(1+\mathrm{i})^2=((1+\mathrm{i})^2)=(2)$.

Wie in (i) wollen wir es noch etwas genauer wissen. Es ist $|\mathbf{Z}[\mathrm{i}]/(1+\mathrm{i})| = |\,\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1+\mathrm{i})| = 2$, also $\mathbf{Z}/(2)\xrightarrow{\sim}\mathbf{Z}[\mathrm{i}]/(1+\mathrm{i})$ und folglich $(1+\mathrm{i})$ ein Primideal in $\mathbf{Z}[\mathrm{i}]$.

Aufgabe 28

Ad (1). Schreibe $\mathfrak{g}=z\mathfrak{a}_0$ und $\mathfrak{h}=w\mathfrak{b}_0$ mit $z,w\in K^\times$ und $\mathfrak{a}_0\,,\,\mathfrak{b}_0\in\mathrm{Ideale}^\times(D)$. Sei $s\in D^\times$ mit $sz\in D^\times$ und $sw\in D^\times$.

Folglich können wir $\mathfrak{g}=\frac{1}{s}sz\mathfrak{a}_0=\frac{1}{s}\mathfrak{a}$ und $\mathfrak{h}=\frac{1}{s}sw\mathfrak{b}_0=\frac{1}{s}\mathfrak{b}$ schreiben, wobei $\mathfrak{a}:=(sz)\mathfrak{a}_0$ und $\mathfrak{b}=(bw)\mathfrak{b}_0$ in $\mathrm{Ideale}^\times(D)$ liegen.

Zeigen wir, daß $\mathfrak{ab}$, $\mathfrak{a}\cap\mathfrak{b}$ *und* $\mathfrak{a}+\mathfrak{b}$ *in* $\mathrm{Ideale}^\times(D)$ *liegen.* Das erledigt im Falle $x=y=s=1$ auch gleich die letzte Frage.

Zu $\mathfrak{ab}$. Es ist $0 \in \mathfrak{ab}$. Sind $d, d' \in D$ und $x, x' \in \mathfrak{ab}$, dann können wir $x = \sum_{i\in[1,n]} a_i b_i$ schreiben mit $n \geqslant 0$, $a_i \in \mathfrak{a}$ und $b_i \in \mathfrak{b}$ für $i \in [1,n]$, und wir können $x' = \sum_{i\in[1,n']} a'_i b'_i$ schreiben mit $n' \geqslant 0$, $a'_i \in \mathfrak{a}$ und $b'_i \in \mathfrak{b}$ für $i \in [1,n']$. Es wird

$$dx + d'x' \;=\; \sum_{i\in[1,n']} (da'_i)b'_i + \sum_{i\in[1,n']} (d'a'_i)b'_i \;\in\; \mathfrak{ab}\,.$$

Ferner ist $(0) \subset \mathfrak{ab}$, da für $a \in \mathfrak{a}^\times$ und $b \in \mathfrak{b}^\times$ dann $ab \in (\mathfrak{ab})^\times$ liegt.

Zu $\mathfrak{a} \cap \mathfrak{b}$. Es ist $0 \in \mathfrak{a} \cap \mathfrak{b}$. Sind $d, d' \in D$ und $x, x' \in \mathfrak{a} \cap \mathfrak{b}$, dann ist auch $dx + d'x' \in \mathfrak{a} \cap \mathfrak{b}$. Ferner ist $(0) \subset \mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Zu $\mathfrak{a} + \mathfrak{b}$. Es ist $0 \in \mathfrak{a} + \mathfrak{b}$. Sind $d, d' \in D$ und $x, x' \in \mathfrak{a} + \mathfrak{b}$, dann können wir $x = a + b$ und $x' = a' + b'$ mit $a, a' \in \mathfrak{a}$ und $b, b' \in \mathfrak{b}$ schreiben. Es wird

$$dx + d'x' \;=\; (da + d'a') + (db + d'b') \;\in\; \mathfrak{a} + \mathfrak{b}\,.$$

Ferner ist $(0) \subset \mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$.

Zeigen wir, daß $\mathfrak{gh}$, $\mathfrak{g} \cap \mathfrak{h}$ *und* $\mathfrak{g} + \mathfrak{h}$ *in* $\mathrm{Ideale}^\times(D)$ *liegen.*

Es ist $\mathfrak{gh} = \mathbf{z}\langle\, \frac{a}{s} \cdot \frac{b}{s} \,:\, a \in \mathfrak{a},\, b \in \mathfrak{b} \,\rangle \;=\; \frac{1}{s^2}(\mathfrak{ab}) \in \underline{\mathrm{Ideale}}^\times(D)$.

Es ist $\mathfrak{g} \cap \mathfrak{h} = \frac{1}{s}\mathfrak{a} \cap \frac{1}{s}\mathfrak{b} = \frac{1}{s}(\mathfrak{a} \cap \mathfrak{b}) \in \underline{\mathrm{Ideale}}^\times(D)$.

Es ist $\mathfrak{g} + \mathfrak{h} = \{\, \frac{a}{s} + \frac{b}{s} \,:\, a \in \mathfrak{a},\, b \in \mathfrak{b} \,\} = \frac{1}{s}(\mathfrak{a} + \mathfrak{b}) \in \underline{\mathrm{Ideale}}^\times(D)$.

Zeigen wir $\mathfrak{g} \overset{!}{\in} \mathrm{Ideale}^\times(D)$, *falls* $\mathfrak{g} \subseteq D$.

Es ist $0 = \frac{1}{s} \cdot 0 \in \mathfrak{g}$.

Seien $d, d' \in D$ und $g, g' \in \mathfrak{g}$. Dann können wir $g = \frac{a}{s}$ und $g' = \frac{a'}{s}$ mit $a, a' \in \mathfrak{a}$ schreiben. Es wird

$$dx + d'x' \;=\; \frac{1}{s}(da + d'a') \;\in\; \frac{1}{s}\mathfrak{a} \;=\; \mathfrak{g}\,.$$

Zeigen wir $\mathfrak{g}^{-1} \overset{!}{\in} \underline{\mathrm{Ideale}}^\times(D)$.

Sei $g \in \mathfrak{g}^\times$. Es ist $\mathfrak{g}^{-1} = g^{-1}g\mathfrak{g}^{-1}$, wobei $g\mathfrak{g}^{-1} \subseteq D$ liegt.

Bleibt $g\mathfrak{g}^{-1} \overset{!}{\in} \mathrm{Ideale}^\times(D)$ zu zeigen. Es ist $0 = g \cdot 0 \in g\mathfrak{g}^{-1}$. Seien $x, x' \in \mathfrak{g}^{-1}$ und $d, d' \in D$ gegeben. Zu zeigen ist $d(gx) + d'(gx') \overset{!}{\in} g\mathfrak{g}^{-1}$. Zu zeigen ist $dx + d'x' \overset{!}{\in} \mathfrak{g}^{-1}$. Sei $h \in \mathfrak{g}$. Zu zeigen ist $(dx + d'x')h \in D$. In der Tat liegen $xh, x'h \in D$ und also liegt auch $(dx + dx')h \in D$.

Ad (2).

Ad $\Leftarrow$. Sei o.E. $\mathfrak{a} \subseteq \mathfrak{p}$. Es ist dann $\mathfrak{ab} \subseteq \mathfrak{a} \subseteq \mathfrak{p}$, da $\mathfrak{a}$ ein Ideal in D ist.

Ad $\Rightarrow$. Annahme, nicht. Dann gibt es ein $a \in \mathfrak{a} \setminus \mathfrak{p}$ und ein $b \in \mathfrak{b} \setminus \mathfrak{p}$. Es ist $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$. Da $\mathfrak{p}$ prim ist, folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Wir haben einen *Widerspruch.*

Aufgabe 29

Schreibe $P := \mathrm{Ideale}^\times_{\mathrm{prim}}(D)$.

Ad (1). Falls $\mathfrak{a} \subseteq \mathfrak{p}^k$ ist, dann ist $\mathfrak{ap}^{-k} \subseteq D$ ein Ideal. Wir können also $\mathfrak{ap}^{-k} = \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\gamma_\mathfrak{q}}$ schreiben, wobei stets $\gamma_\mathfrak{q} \geqslant 0$ ist und $\{\, \mathfrak{p} \in P \,:\, \gamma_\mathfrak{p} > 0 \,\}$ endlich ist; cf. Satz 63.(1).

Folglich ist $\mathfrak{a} = \mathfrak{ap}^{-k}\mathfrak{p}^k = \mathfrak{p}^{k+\gamma_\mathfrak{p}} \cdot \prod_{\mathfrak{q}\in P\setminus\{\mathfrak{p}\}} \mathfrak{q}^{\gamma_\mathfrak{q}}$. Somit ist $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) = k + \gamma_\mathfrak{p} \geqslant k$; cf. Lemma 65.

Sei umgekehrt $\mathrm{v}_\mathfrak{p}(\mathfrak{a}) \geqslant k$. Es ist

$$\mathfrak{a} \;=\; \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\mathrm{v}_\mathfrak{q}(\mathfrak{a})} \;=\; \mathfrak{p}^k \cdot \mathfrak{p}^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})-k} \cdot \prod_{\mathfrak{q}\in P\smallsetminus\{\mathfrak{p}\}} \mathfrak{q}^{\mathrm{v}_\mathfrak{q}(\mathfrak{a})} \;\subseteq\; \mathfrak{p}^k \,.$$

Alternativ kann man auch Bemerkung 66.(1) auf $\mathfrak{a}\mathfrak{p}^{-k}$ anwenden.

Ad (2). Seien $(\alpha_\mathfrak{q})_\mathfrak{q}$, $(\beta_\mathfrak{q})_\mathfrak{q} \in \mathbf{Z}^{\oplus P}$. Merken wir zunächst an, daß genau dann $\prod_{\mathfrak{q}\in P} \mathfrak{q}^{\alpha_\mathfrak{q}} \subseteq \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\beta_\mathfrak{q}}$ liegt, wenn $\prod_{\mathfrak{q}\in P} \mathfrak{q}^{\alpha_\mathfrak{q}-\beta_\mathfrak{q}} \subseteq D$ liegt, i.e. wenn $\alpha_\mathfrak{p} \geqslant \beta_\mathfrak{p}$ ist für $\mathfrak{p} \in P$; cf. Bemerkung 66.(1).

Es ist $\mathfrak{g}\mathfrak{h} = \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\mathrm{v}_\mathfrak{q}(\mathfrak{g})+\mathrm{v}_\mathfrak{q}(\mathfrak{h})}$. Folglich ist $\mathrm{v}_\mathfrak{p}(\mathfrak{g}\mathfrak{h}) = \mathrm{v}_\mathfrak{p}(\mathfrak{g}) + \mathrm{v}_\mathfrak{p}(\mathfrak{h}) = \gamma + \chi$.

Da $\mathfrak{g}\mathfrak{g}^{-1} = (1)$, folgt hieraus $\mathrm{v}_\mathfrak{p}(\mathfrak{g}) + \mathrm{v}_\mathfrak{p}(\mathfrak{g}^{-1}) = 0$, i.e. $\mathrm{v}_\mathfrak{p}(\mathfrak{g}^{-1}) = -\gamma$.

Es ist $\mathfrak{g} \cap \mathfrak{h}$ das terminale gebrochene Ideal, das in $\mathfrak{g}$ und $\mathfrak{h}$ enthalten ist. Dies trifft nach der Anmerkung eingangs und nach Lemma 65 auch auf $\prod_{\mathfrak{q}\in P} \mathfrak{q}^{\max\{\mathrm{v}_\mathfrak{q}(\mathfrak{g}),\mathrm{v}_\mathfrak{q}(\mathfrak{h})\}}$ zu. Also ist $\mathfrak{g} \cap \mathfrak{h} = \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\max\{\mathrm{v}_\mathfrak{q}(\mathfrak{g}),\mathrm{v}_\mathfrak{q}(\mathfrak{h})\}}$. Insbesondere ist $\mathrm{v}_\mathfrak{p}(\mathfrak{g} \cap \mathfrak{h}) = \max\{\mathrm{v}_\mathfrak{p}(\mathfrak{g}), \mathrm{v}_\mathfrak{p}(\mathfrak{h})\} = \max\{\gamma, \chi\}$.

Es ist $\mathfrak{g}+\mathfrak{h}$ das initiale gebrochene Ideal, das $\mathfrak{g}$ und $\mathfrak{h}$ enthält. Dies trifft nach der Anmerkung eingangs und nach Lemma 65 auch auf $\prod_{\mathfrak{q}\in P} \mathfrak{q}^{\min\{\mathrm{v}_\mathfrak{q}(\mathfrak{g}),\mathrm{v}_\mathfrak{q}(\mathfrak{h})\}}$ zu. Also ist $\mathfrak{g} + \mathfrak{h} = \prod_{\mathfrak{q}\in P} \mathfrak{q}^{\min\{\mathrm{v}_\mathfrak{q}(\mathfrak{g}),\mathrm{v}_\mathfrak{q}(\mathfrak{h})\}}$. Insbesondere ist $\mathrm{v}_\mathfrak{p}(\mathfrak{g} + \mathfrak{h}) = \min\{\mathrm{v}_\mathfrak{p}(\mathfrak{g}), \mathrm{v}_\mathfrak{p}(\mathfrak{h})\} = \min\{\gamma, \chi\}$.

Ad (3). Es ist $\mathrm{v}_\mathfrak{p}(xy) = \mathrm{v}_\mathfrak{p}(\,(xy)\,) = \mathrm{v}_\mathfrak{p}(\,(x)(y)\,) \overset{(2)}{=} \mathrm{v}_\mathfrak{p}(\,(x)\,) + \mathrm{v}_\mathfrak{p}(\,(y)\,) = \mathrm{v}_\mathfrak{p}(x) + \mathrm{v}_\mathfrak{p}(y)$.

Daraus folgt übrigens auch $0 = \mathrm{v}_\mathfrak{p}(1) = \mathrm{v}_\mathfrak{p}(xx^{-1}) = \mathrm{v}_\mathfrak{p}(x) + \mathrm{v}_\mathfrak{p}(x^{-1})$, i.e. $\mathrm{v}_\mathfrak{p}(x^{-1}) = -\,\mathrm{v}_\mathfrak{p}(x)$.

Es ist $x+y \in (x,y)$, also $(x+y) \subseteq (x,y) = (x)+(y)$ und somit $\mathrm{v}_\mathfrak{p}(x+y) = \mathrm{v}_\mathfrak{p}(\,(x+y)\,) \overset{(1)}{\geqslant} \mathrm{v}_\mathfrak{p}(\,(x)+(y)\,) \overset{(2)}{=} \min\{\mathrm{v}_\mathfrak{p}(\,(x)\,), \mathrm{v}_\mathfrak{p}(\,(y)\,)\} = \min\{\mathrm{v}_\mathfrak{p}(x), \mathrm{v}_\mathfrak{p}(y)\}$.

Sei nun o.E. $\mathrm{v}_\mathfrak{p}(x) > \mathrm{v}_\mathfrak{p}(y)$. Es ist $\mathrm{v}_\mathfrak{p}(x+y) \geqslant \mathrm{v}_\mathfrak{p}(y)$. Wir haben $\mathrm{v}_\mathfrak{p}(x+y) \overset{!}{=} \mathrm{v}_\mathfrak{p}(y)$ zu zeigen. *Annahme,* es ist $\mathrm{v}_\mathfrak{p}(x+y) > \mathrm{v}_\mathfrak{p}(y)$. Dann ist

$$\mathrm{v}_\mathfrak{p}(y) \;=\; \mathrm{v}_\mathfrak{p}(x+y+(-x)) \;\geqslant\; \min\{\mathrm{v}_\mathfrak{p}(x+y), \mathrm{v}_\mathfrak{p}(-x)\} \;=\; \min\{\mathrm{v}_\mathfrak{p}(x+y), \mathrm{v}_\mathfrak{p}(x)\} \;>\; \mathrm{v}_\mathfrak{p}(y)\,,$$

und wir haben einen *Widerspruch.*

Ad (4). Dank (2) und Lemma 65 ist genau dann $\mathfrak{a} + \mathfrak{b} = (1)$, wenn $\mathrm{v}_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathrm{v}_\mathfrak{p}(\mathfrak{a}), \mathrm{v}_\mathfrak{p}(\mathfrak{b})\}$ gleich $\mathrm{v}_\mathfrak{p}(\,(1)\,) = 0$ ist für $\mathfrak{p} \in P$. Da alle Bewertungen von $\mathfrak{a}$ und $\mathfrak{b}$ in $\mathbf{Z}_{\geqslant 0}$ liegen nach Bemerkung 66.(1), folgt $(\mathrm{v}_\mathfrak{p}(\mathfrak{a}) = 0$ oder $\mathrm{v}_\mathfrak{p}(\mathfrak{b}) = 0)$ für $\mathfrak{p} \in P$. Dies ist genau dann der Fall, wenn kein $\mathfrak{p} \in P$ sowohl in der Primidealfaktorzerlegung von $\mathfrak{a}$ als auch in der von $\mathfrak{b}$ als Faktor auftritt.

Ad (5). Sei $P_1 := \{\, \mathfrak{q} \in P \,:\, \mathrm{v}_\mathfrak{q}(\mathfrak{a}) \geqslant 1 \,\}$. Es ist P_1 eine endliche Menge. Sei mit Lemma 71 ein Element $x \in D$ mit $\mathrm{v}_\mathfrak{q}(x) = \mathrm{v}_\mathfrak{q}(\mathfrak{a})$ für $\mathfrak{q} \in P_1$ gefunden.

Sei $P_2 := \{\, \mathfrak{q} \in P \,:\, \mathrm{v}_\mathfrak{q}(\mathfrak{a}) = 0$ und $\mathrm{v}_\mathfrak{q}(x) \geqslant 1 \,\}$. Es ist P_2 eine endliche Menge mit $P_1 \cap P_2 = \emptyset$. Sei mit Lemma 71 ein Element $y \in D$ mit $\mathrm{v}_\mathfrak{q}(y) = \mathrm{v}_\mathfrak{q}(\mathfrak{a})$ für $\mathfrak{q} \in P_1$ und $\mathrm{v}_\mathfrak{q}(y) = 0$ für $\mathfrak{q} \in P_2$ gefunden.

Wir wollen $\mathfrak{a} \overset{!}{=} (x,y)$ zeigen. Dank Lemma 65 genügt es, $\mathrm{v}_\mathfrak{q}(\mathfrak{a}) \overset{!}{=} \mathrm{v}_\mathfrak{q}(\,(x,y)\,) = \mathrm{v}_\mathfrak{q}(\,(x) + (y)\,)$ für $\mathfrak{q} \in P$ zu zeigen. Dank (2) bedeutet das, $\mathrm{v}_\mathfrak{q}(\mathfrak{a}) \overset{!}{=} \min\{\mathrm{v}_\mathfrak{q}(x), \mathrm{v}_\mathfrak{q}(y)\}$ zu zeigen.

Fall $\mathfrak{q} \in P_1$. Es ist $\min\{\mathrm{v}_\mathfrak{q}(x), \mathrm{v}_\mathfrak{q}(y)\} = \min\{\mathrm{v}_\mathfrak{q}(\mathfrak{a}), \mathrm{v}_\mathfrak{q}(\mathfrak{a})\} = \mathrm{v}_\mathfrak{q}(\mathfrak{a})$.

Fall $\mathfrak{q} \in P_2$. Es ist $\min\{\mathrm{v}_\mathfrak{q}(x), \mathrm{v}_\mathfrak{q}(y)\} = \min\{\mathrm{v}_\mathfrak{q}(x), 0\} = 0 = \mathrm{v}_\mathfrak{q}(\mathfrak{a})$.

Fall $\mathfrak{q} \in P \smallsetminus (P_1 \sqcup P_2)$. Es ist $\min\{\mathrm{v}_\mathfrak{q}(x), \mathrm{v}_\mathfrak{q}(y)\} = \min\{0, \mathrm{v}_\mathfrak{q}(y)\} = 0 = \mathrm{v}_\mathfrak{q}(\mathfrak{a})$.

Ad (6). Gemäß (2) und (4) ist $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$, denn für $\mathfrak{q} \in P$ folgt aus $\mathrm{v}_\mathfrak{q}(\mathfrak{a}) = 0$ oder $\mathrm{v}_\mathfrak{q}(\mathfrak{b}) = 0$, daß $\mathrm{v}_\mathfrak{q}(\mathfrak{a}) + \mathrm{v}_\mathfrak{q}(\mathfrak{b}) = \max\{\mathrm{v}_\mathfrak{q}(\mathfrak{a}), \mathrm{v}_\mathfrak{q}(\mathfrak{b})\}$ ist.

Betrachte die exakte Sequenz D-linearer Abbildungen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{ab} & \xrightarrow{\iota} & \mathfrak{a}\oplus\mathfrak{b} & \xrightarrow{\varphi} & D & \longrightarrow & 0 \\ & & x & \longmapsto & (x,-x) & & & & \\ & & & & (a,b) & \longmapsto & a+b & & \end{array}$$

Hierbei ist φ surjektiv wegen $\mathfrak{a}+\mathfrak{b}=D$. Ist $\varphi((a,b))=0$, dann ist $a=-b=:x\in\mathfrak{a}\cap\mathfrak{b}=\mathfrak{ab}$, also $(a,b)=(x,-x)=\iota(x)$. Umgekehrt ist für $x\in\mathfrak{ab}$ auch $\varphi(\iota(x))=\varphi((x,-x))=x+(-x)=0$.

Da $\mathfrak{a}+\mathfrak{b}=(1)$, gibt es $a_1\in\mathfrak{a}$ und $b_1\in\mathfrak{b}$ mit $a_1+b_1=1$. Sei $D\xrightarrow{\sigma}\mathfrak{a}\oplus\mathfrak{b}$, $d\mapsto(\,da_1\,,\,db_1\,)$. Es ist $\varphi\circ\sigma=\mathrm{id}_D$. Definiere die D-lineare Abbildung $\mathfrak{a}\oplus\mathfrak{b}\xrightarrow{\psi}\mathfrak{ab}$, $(a,b)\mapsto x$ mit $\iota(x)=(a,b)-\sigma(\varphi((a,b)))=(a-(a+b)a_1,b-(a+b)b_1)$, i.e. $\psi((a,b))=a-(a+b)a_1=-b+(a+b)b_1$.

Definiere die D-lineare Abbildung $\mathfrak{a}\oplus\mathfrak{b}\xrightarrow{\alpha}D\oplus\mathfrak{ab}$, $(a,b)\mapsto(\varphi((a,b)),\psi((a,b)))$.

Definiere die D-lineare Abbildung $D\oplus\mathfrak{ab}\xrightarrow{\beta}\mathfrak{a}\oplus\mathfrak{b}$, $(d,x)\mapsto\sigma(d)+\iota(x)$.

Für $(d,x)\in D\oplus\mathfrak{ab}$ ist

$$\begin{aligned} \alpha(\beta((d,x))) &= \alpha(\sigma(d)+\iota(x)) \\ &= (\varphi(\sigma(d)+\iota(x)),\psi(\sigma(d)+\iota(x))) \\ &= (\varphi((da_1+x,db_1-x)),\psi((da_1+x,db_1-x))) \\ &= (da_1+x+db_1-x,da_1+x-(da_1+x+db_1-x)a_1) \\ &= (d,x)\,. \end{aligned}$$

Für $(a,b)\in\mathfrak{a}\oplus\mathfrak{b}$ ist

$$\begin{aligned} \beta(\alpha((a,b))) &= \beta((\varphi((a,b)),\psi((a,b)))) \\ &= \sigma(\varphi((a,b)))+\iota(\psi((a,b))) \\ &= \sigma(a+b)+\iota(a-(a+b)a_1) \\ &= (\,(a+b)a_1\,,\,(a+b)b_1\,)+(\,a-(a+b)a_1\,,\,-a+(a+b)a_1\,) \\ &= (a,b)\,. \end{aligned}$$

Also sind α und β sich invertierende Isomorphismen von D-Moduln.

Ad (7). Zeigen wir $\mathfrak{a}\oplus\mathfrak{a}^{-1}\simeq D\oplus D$. Für $x\in K^\times$ ist $\mathfrak{a}^{-1}$ isomorph zu $x\mathfrak{a}^{-1}$. Also genügt es zu zeigen, daß es ein $x\in K^\times$ gibt mit $\mathfrak{a}\oplus x\mathfrak{a}^{-1}$ isomorph zu $D\oplus D$.

Mit Lemma 71 können wir ein $x\in D^\times$ so wählen, daß $\mathrm{v}_\mathfrak{p}(x)=\mathrm{v}_\mathfrak{p}(\mathfrak{a})$ ist für $\mathfrak{p}\in P$ mit $\mathrm{v}_\mathfrak{p}(\mathfrak{a})\geqslant 1$. Dann ist $\mathrm{v}_\mathfrak{p}(x\mathfrak{a}^{-1})\geqslant 0$ für $\mathfrak{p}\in P$, also $x\mathfrak{a}^{-1}\in\mathrm{Ideale}^\times(D)$. Ferner ist $\mathrm{v}_\mathfrak{p}(x\mathfrak{a}^{-1})=0$, wann immer $\mathrm{v}_\mathfrak{p}(\mathfrak{a})\geqslant 1$ ist. Also ist $\mathfrak{a}+x\mathfrak{a}^{-1}=(1)$; cf. (4). Folglich ist

$$\mathfrak{a}\oplus x\mathfrak{a}^{-1}\overset{(6)}{\simeq}D\oplus\mathfrak{a}\cdot x\mathfrak{a}^{-1}=D\oplus(x)\simeq D\oplus D\,.$$

Annahme, es ist $\mathfrak{a}$ in eine direkte Summe von echten D-Teilmoduln zerlegbar, sagen wir, $\mathfrak{a}=\mathfrak{x}\oplus\mathfrak{y}$ mit $\mathfrak{x}\neq(0)$ und $\mathfrak{y}\neq(0)$. Wähle $x\in\mathfrak{x}^\times$ und $y\in\mathfrak{y}^\times$. Es wird $xy\in\mathfrak{x}\cap\mathfrak{y}=(0)$, also $xy=0$, im *Widerspruch* zu D Integritätsbereich. Man sagt, $\mathfrak{a}$ ist *unzerlegbar.*

> Auch alle gebrochenen Ideale von D sind unzerlegbar als D-Moduln, da jedes gebrochene Ideal isomorph zu einem Ideal ist.

Ist $\mathfrak{a}$ ein Hauptideal, sagen wir $\mathfrak{a}=(a)$ mit $a\in D^\times$, dann ist D isomorph zu $\mathfrak{a}$, indem d auf da geschickt wird.

Ist umgekehrt ein Isomorphismus $D \xrightarrow{\sim} \mathfrak{a}$ gegeben, dann sei $1 \mapsto a \in D^\times$. Folglich ist das Bild gleich (a). Wegen Surjektivität ist also $(a) = \mathfrak{a}$.

Somit ist $\mathfrak{a} \simeq D$ genau dann, wenn $\mathfrak{a}$ ein Hauptideal ist.

> Ist $\mathfrak{a}$ kein Hauptideal, dann ist mithin die Zerlegung von $D^{\oplus 2}$ in unzerlegbare Summanden nicht auf bis auf Reihenfolge eindeutige Weise gegeben. Man sagt, die *Krull-Schmidt-Eigenschaft* ist in den endlich erzeugten D-Moduln verletzt, falls D kein Hauptidealbereich ist.

Ad (8).

Zeigen wir $S^{-1}(\mathfrak{ab}) \stackrel{!}{=} (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$. Die linke Seite ist $\mathbf{Z}$-linear erzeugt von Elementen der Form $s^{-1}ab$ mit $s \in S$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Diese liegen in der rechten Seite. Die rechte Seite ist $\mathbf{Z}$-linear erzeugt von Elementen der Form $s^{-1}at^{-1}b$ mit $s, t \in S$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Diese liegen in der linken Seite.

Zeigen wir $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) \stackrel{!}{=} (S^{-1}\mathfrak{a}) \cap (S^{-1}\mathfrak{b})$. Ein Element $x \in K$ liegt genau dann in der linken Seite, wenn es ein $s \in S$ mit $sx \in \mathfrak{a} \cap \mathfrak{b}$ gibt. Dann liegt es aber in der rechten Seite. Ein Element $y \in K$ liegt in der rechten Seite, wenn es ein $s \in S$ mit $sy \in \mathfrak{a}$ und ein $t \in S$ mit $ty \in \mathfrak{b}$ gibt. Dann aber ist $sty \in \mathfrak{a} \cap \mathfrak{b}$ und somit y in der linken Seite enthalten.

Zeigen wir $S^{-1}(\mathfrak{a} + \mathfrak{b}) \stackrel{!}{=} (S^{-1}\mathfrak{a}) + (S^{-1}\mathfrak{b})$. Ein Element der linken Seite ist von der Form $s^{-1}(a+b) = s^{-1}a + s^{-1}b$ mit $s \in S$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, liegt also in der rechten Seite. Ein Element der rechten Seite ist von der Form $s^{-1}a + t^{-1}b = (s^{-1}t^{-1})(ta + sb)$ mit $s, t \in S$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, liegt also in der linken Seite.

Zeigen wir $\mathfrak{a}_\mathfrak{p} \stackrel{!}{=} (\mathfrak{p}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})}$. Es ist $\mathfrak{a} = \prod_{\mathfrak{q} \in P} \mathfrak{q}^{\mathrm{v}_\mathfrak{q}(\mathfrak{a})}$ und also $\mathfrak{a}_\mathfrak{q} = \prod_{\mathfrak{q} \in P} (\mathfrak{q}_\mathfrak{q})^{\mathrm{v}_\mathfrak{q}(\mathfrak{a})}$. Somit müssen wir $\mathfrak{q}_\mathfrak{p} \stackrel{!}{=} (1)$ für $\mathfrak{q} \in P \smallsetminus \{\mathfrak{p}\}$ zeigen. Da $\mathfrak{q}$ ein von $\mathfrak{p}$ verschiedenes maximales Ideal von D ist, ist $\mathfrak{q} \not\subseteq \mathfrak{p}$. Also gibt es ein $q \in \mathfrak{q} \smallsetminus \mathfrak{p}$. Es ist $q \in \mathrm{U}(D_\mathfrak{p}) \cap \mathfrak{q}_\mathfrak{p}$. Folglich ist $(1) = (q) \subseteq \mathfrak{q}_\mathfrak{p} \subseteq (1)$ in $D_\mathfrak{p}$, i.e. $\mathfrak{q}_\mathfrak{p} = (1)$.

Aufgabe 30

Ad (1). Es ist $0 \in \mathfrak{ac}$. Es ist $\mathfrak{ac}$ unter Summen abgeschlossen. Sei $x \in \mathfrak{ac}$, sei $c \in C$. Schreibe $x = \sum_{i \in [1,k]} z_i a_i c_i$ mit $k \geqslant 0$ und $z_i \in \mathbf{Z}$, $a_i \in \mathfrak{a}$, $c_i \in \mathfrak{c}$ für $i \in [1,k]$. Es wird $cx = \sum_{i \in [1,k]} z_i a_i (cc_i) \in \mathfrak{ac}$.

Ad (2).

Ad (i). Sei $n := \deg(\mu_{b,K}(X))$.

Schreibe

$$\mathfrak{k} \;:=\; (\mu_{b,k}(X)) + \mathfrak{a} \cdot A[X] \;\subseteq\; A[X]\,.$$

1. Betrachte den surjektiven Ringmorphismus

$$\begin{array}{rcl} A[X] & \xrightarrow{\hat{\eta}} & A[b]/(\mathfrak{a} \cdot A[b]) \\ a & \longmapsto & a + (\mathfrak{a} \cdot A[b]) \\ X & \longmapsto & b + (\mathfrak{a} \cdot A[b])\,; \end{array}$$

cf. **[5,** §1.6.2].

Es liegt $\mathfrak{k}$ im Kern von $\hat{\eta}$.

Werde umgekehrt $f(X) \in A[X]$ unter $\hat{\eta}$ auf 0 abgebildet, i.e. liege $f(b) \in \mathfrak{a} \cdot A[b]$.

Es ist das K-linear unabhängige Tupel $(\, b^i \,:\, i \in [0, n-1]\,)$ eine A-lineare Basis von $A[b]$.

Schreibe mit Polynomdivision $f(X) = \mu_{b,K}(X) \cdot q(X) + r(X)$ mit $q(X), r(X) \in A[X]$ und mit $(r(X) = 0$ oder $(r(X) \neq 0$ und $\deg(r) \in [0, n-1]))$. Schreibe $r(X) =: \sum_{i \in [0,n-1]} u_i X^i$ mit $u_i \in A$ für $i \in [0, n-1]$.

Es ist $\mathfrak{a} \cdot A[b] = \{\, \sum_{i \in [0,n-1]} a_i\, b^i \;:\; a_i \in \mathfrak{a}\,\}$.

Es ist $\sum_{i\in[0,n-1]} u_i b^i = r(b) = f(b) \in \mathfrak{a}\cdot A[b]$. Also ist $\sum_{i\in[0,n-1]} u_i b^i = \sum_{i\in[0,n-1]} a_i\, b^i$ für gewisse $a_i \in \mathfrak{a}$ für $i \in [0, n-1]$. Koeffizientenvergleich gibt $u_i \in \mathfrak{a}$ für $i \in [0, n-1]$.

Folglich ist $f(X) = \mu_{b,K}(X)\cdot q(X) + r(X) \in (\mu_{b,k}(X)) + \mathfrak{a}\cdot A[X] = \mathfrak{k}$.

Insgesamt ist $\mathfrak{k} = \mathrm{Kern}(\hat{\eta})$. Wir erhalten mit **[5,** §1.4.3] den Ringisomorphismus

$$\begin{array}{rcl} A[X]/\mathfrak{k} & \xrightarrow[\sim]{\eta} & A[b]/(\mathfrak{a}\cdot A[b]) \\ f(X)+\mathfrak{k} & \longmapsto & f(b)+(\mathfrak{a}\cdot A[b])\,. \end{array}$$

2. Betrachte den surjektiven Ringmorphismus

$$\begin{array}{rcl} A[X] & \xrightarrow{\hat{\psi}} & \bar{A}[X]/(\bar{\mu}_{b,K}(X)) \\ a & \longmapsto & \bar{a}+(\bar{\mu}_{b,K}(X)) \\ X & \longmapsto & X+(\bar{\mu}_{b,K}(X))\,; \end{array}$$

cf. **[5,** §1.6.2].

Es liegt $\mathfrak{k}$ im Kern von $\hat{\psi}$.

Werde umgekehrt $f(X) \in A[X]$ unter $\hat{\psi}$ auf 0 abgebildet, i.e. liege $\bar{f}(X) \in (\bar{\mu}_{b,K}(X))$.

Dann können wir $\bar{f}(X) = \bar{\mu}_{b,K}(X)\cdot \bar{s}(X)$ schreiben für ein $s(X) \in A[X]$. Dann wird $f(X) = \mu_{b,K}(X)\cdot s(X) + t(X)$ für ein $t(X) \in \mathfrak{a}\cdot A[X]$.

Also ist $f(X) \in (\mu_{b,k}(X)) + \mathfrak{a}\cdot A[X] = \mathfrak{k}$.

Insgesamt ist $\mathfrak{k} = \mathrm{Kern}(\hat{\psi})$. Wir erhalten mit **[5,** §1.4.3] den Ringisomorphismus

$$\begin{array}{rcl} A[X]/\mathfrak{k} & \xrightarrow[\sim]{\psi} & \bar{A}[X]/(\bar{\mu}_{b,K}(X)) \\ f(X)+\mathfrak{k} & \longmapsto & \bar{f}(X)+(\bar{\mu}_{b,K}(X))\,. \end{array}$$

3. Setzen wir $\varphi := \psi\circ\eta^{-1}$, so erhalten wir den Ringisomorphismus

$$\begin{array}{rcl} A[b]/(\mathfrak{a}\cdot A[b]) & \xrightarrow[\sim]{\varphi} & \bar{A}[X]/(\bar{\mu}_{b,K}(X)) \\ f(b)+(\mathfrak{a}\cdot A[b]) & \longmapsto & \bar{f}(X)+(\bar{\mu}_{b,K}(X))\,. \end{array}$$

Die Ideale von $A[b]$, die $\mathfrak{a}$ enthalten, stehen in Bijektion zu den Idealen von $A[b]/(\mathfrak{a}\cdot A[b])$ via Restklassenmorphismus.

Diese stehen in Bijektion zu den Idealen von $\bar{A}[X]/(\bar{\mu}_{b,K}(X))$ via φ.

Ad (ii). Wir wollen Aufgabe 26 verwenden. Dazu bemerken wir, daß $(\bar{u}_i(X)^{\alpha_i})+(\bar{u}_j(X)^{\alpha_j}) = (1)$ für $i,\ j \in [1,k]$ mit $i \neq j$ gemäß Aufgabe 29.(4). Ferner ist $(\bar{\mu}_{b,K}(X)) = \bigcap_{i\in[1,k]}(\bar{u}_i(X)^{\alpha_i})$ gemäß Aufgabe 29.(2) und Lemma 65.

Mit Aufgabe 26 und **[5,** §1.4.3] erhalten wir so den Ringisomorphismus

$$\begin{array}{rcl} \bar{A}[X]/(\bar{\mu}_{b,K}(X)) & \xrightarrow[\sim]{\zeta} & \prod_{i\in[1,k]} \bar{A}[X]/(\bar{u}_i(X)^{\alpha_i}) \\ \bar{f}(X)+(\bar{\mu}_{b,K}(X)) & \longmapsto & (\bar{f}(X)+(\bar{u}_i(X)^{\alpha_i}))_{i\in[1,k]}\,. \end{array}$$

Es hat $R_i := \bar{A}[X]/(\bar{u}_i(X)^{\alpha_i})$ nur das maximale Ideal $\mathfrak{m}_i := (\bar{u}_i(X))/(\bar{u}_i(X)^{\alpha_i})$, für $i \in [1,k]$.

Für $f(X) \in A[X]$ ist genau dann $\bar{f}(X)+(\bar{u}_i(X)^{\alpha_i}) \in \mathfrak{m}_i$, wenn $\bar{f}(X) \in (\bar{u}_i(X))$ liegt.

Also hat die rechte Seite $R_1\times\cdots\times R_k$ genau die maximalen Ideale

$$\tilde{\mathfrak{m}}_i \;:=\; R_1\times\cdots\times R_{i-1}\times\mathfrak{m}_i\times R_{i+1}\times\cdots\times R_k$$

für $i \in [1,k]$. Denn ein maximales Ideal $\mathfrak{n}$ in diesem direkten Produkt kann nicht alle Tupel enthalten, die an einer Stelle eine 1 und ansonsten Nullen aufweisen. Sei o.E. $(1,0,\ldots,0) \notin \mathfrak{n}$. Dann ist

$$\mathfrak{n} \;\subseteq\; \mathfrak{n} + (0 \times R_2 \times \cdots \times R_k) \;\subset\; R_1 \times \cdots \times R_k \;,$$

da auch $(1,0,\ldots,0) \notin \mathfrak{n} + (0 \times R_2 \times \cdots \times R_k)$, denn läge ein Element der Form $(1,*,\ldots,*)$ in $\mathfrak{n}$, dann wegen $\mathfrak{n}$ Ideal auch $(1,0,\ldots,0)$. Wegen Maximalität von $\mathfrak{n}$ folgt $(0 \times R_2 \times \cdots \times R_k) \subseteq \mathfrak{n}$. Bezeichnet $\mathfrak{m}$ das Bild der Projektion von $\mathfrak{n}$ auf R_1, dann ist deswegen $\mathfrak{n} = \mathfrak{m} \times R_2 \times \cdots \times R_k$. Da

$$(R_1 \times R_2 \times \cdots \times R_k)/(\mathfrak{m} \times R_2 \times \cdots \times R_k) \;\simeq\; R_1/\mathfrak{m}$$

ein Körper ist, ist $\mathfrak{m} \subset R_1$ maximal und also $\mathfrak{m} = \mathfrak{m}_1$.

Sei $i \in [1,k]$ gegeben. Es ist $\zeta^{-1}(\tilde{\mathfrak{m}}_i) = (\bar{u}_i(X))/(\bar{\mu}_{b,K}(X))$.

Sodann ist $\varphi^{-1}(\zeta^{-1}(\tilde{\mathfrak{m}}_i)) = (u_i(b) + (\mathfrak{a} \cdot A[b]))$.

Schließlich ist das Urbild dieses Ideals in $A[b]$ gegeben durch $(u_i(b)) + \mathfrak{a}A[b]$.

Somit sind die maximalen Ideale über $\mathfrak{a}$ in $A[b]$ gegeben durch $\mathfrak{q}_i := (u_i(b)) + \mathfrak{a}A[b]$ für $i \in [1,k]$. Desweiteren ist $A[b]/\mathfrak{q}_i \xrightarrow{\sim} \bar{A}[X]/(\bar{u}_i(X))$, $b + \mathfrak{q}_i \mapsto X + (\bar{u}_i(X))$ dank (i) und also

$$[A[b]/\mathfrak{q}_i : \bar{A}] \;=\; [\bar{A}[X]/(\bar{u}_i(X)) : \bar{A}] \;=\; \deg(\bar{u}_i)$$

für $i \in [1,k]$.

Ad (iii). Nun ist $A[b] = B$ vorausgesetzt. Insbesondere ist $A[b]$ ein Dedekindbereich.

Dann ist $\mathfrak{a} \cdot B = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_k^{\beta_k}$ mit $\beta_i := \mathrm{v}_{\mathfrak{q}_i}(\mathfrak{a}) \geqslant 1$ für $i \in [1,k]$; cf. Aufgabe 29.(1).

Sei $i \in [1,k]$ gegeben. Wir wollen den Exponenten β_i bestimmen. Sei o.E. $i = 1$.

Sei $s \geqslant 0$. Das Bild $\bar{\mathfrak{q}}_1^s$ von $\mathfrak{q}_1^s$ in $B/(\mathfrak{a} \cdot B)$ ist gleich $(\mathfrak{q}_1^s + (\mathfrak{a} \cdot B))/(\mathfrak{a} \cdot B)$, mit Aufgabe 29.(2) also gleich $\mathfrak{q}_1^{\min\{\beta_1\,,\,s\}}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_k^{\beta_k}/(\mathfrak{a} \cdot B)$. Somit haben wir

$$\bar{\mathfrak{q}}_1^0 \supset \ldots \supset \bar{\mathfrak{q}}_1^{\beta_1 - 1} \;\supset\; \bar{\mathfrak{q}}_1^{\beta_1} \;=\; \bar{\mathfrak{q}}_1^{\beta_1 + 1} \;=\; \ldots$$

Das übersetzt sich via $\zeta \circ \varphi$ zu

$$\tilde{\mathfrak{m}}_1^0 \supset \ldots \supset \tilde{\mathfrak{m}}_1^{\beta_1 - 1} \;\supset\; \tilde{\mathfrak{m}}_1^{\beta_1} \;=\; \tilde{\mathfrak{m}}_1^{\beta_1 + 1} \;=\; \ldots$$

Auf der anderen Seite ist nach Konstruktion aber

$$\tilde{\mathfrak{m}}_1^0 \supset \ldots \supset \tilde{\mathfrak{m}}_1^{\alpha_1 - 1} \;\supset\; \tilde{\mathfrak{m}}_1^{\alpha_1} \;=\; \tilde{\mathfrak{m}}_1^{\alpha_1 + 1} \;=\; \ldots$$

Also ist $\alpha_1 = \beta_1$.

Im Ergebnis ist mithin

$$\mathfrak{a} \cdot A[b] \;=\; \mathfrak{q}_1^{\alpha_1}\mathfrak{q}_2^{\alpha_2} \cdots \mathfrak{q}_k^{\alpha_k} \;.$$

Ad (3). Es ist $\mu_{\sqrt{d},\mathbf{Q}}(X) = X^2 - d$. Schreibe $\bar{z} := z + p\mathbf{Z} \in \mathbf{F}_p$ für $z \in \mathbf{Z}$; analog für Polynome mit Koeffizienten in $\mathbf{Z}$.

Fall $d \equiv_4 2$ *oder* $d \equiv_4 3$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\sqrt{d}]$; cf. Aufgabe 3. Es ist $\mu_{\sqrt{d},\mathbf{Q}}(X) = X^2 - d$.

Unterfall $p = 2$. Es ist $X^2 - \bar{d} = (X - \bar{d})^2 \in \mathbf{F}_2[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(2) \;=\; 2\mathbf{Z}[\sqrt{d}] \;=\; (2, \sqrt{d} - d)^2 \;.$$

Speziell ergibt sich für $d = -1$ die Primidealfaktorzerlegung $(2) = (2, 1 + \mathrm{i})^2 = (1 + \mathrm{i})^2$.

Unterfall $p \neq 2$ *und* $\bar{d} \in (\mathbf{F}_p^\times)^2$. Wähle $s \in \mathbf{Z}$ mit $s^2 \equiv_p d$. Es ist $X^2 - \bar{d} = (X - \bar{s})(X + \bar{s}) \in \mathbf{F}_p[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(p) \;=\; p\mathbf{Z}[\sqrt{d}] \;=\; (p, \sqrt{d} - s)^1 (p, \sqrt{d} + s)^1 \;.$$

Speziell ergibt sich für $d = -1$ die Primidealfaktorzerlegung $(5) = (5, \mathrm{i} + 2)^1 (5, \mathrm{i} - 2)^1 = (\mathrm{i} + 2)^1 (\mathrm{i} - 2)^1$.

Unterfall $p \neq 2$ *und* $\bar{d} \notin (\mathbf{F}_p^\times)^2$. Es ist $X^2 - \bar{d} \in \mathbf{F}_p[X]$ irreduzibel. Wir erhalten die triviale Primidealfaktorzerlegung

$$(p) \;=\; p\mathbf{Z}[\sqrt{d}] \;=\; (p)^1 \;.$$

Speziell ergibt sich für $d = -1$ die triviale Primidealfaktorzerlegung $(3) = (3)^1$.

Fall $d \equiv_4 1$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\alpha]$ mit $\alpha := \frac{1}{2}(1 + \sqrt{d})$; cf. Aufgabe 3. Schreibe $t := \frac{d-1}{4}$. Es ist $\mu_{\alpha,\mathbf{Q}}(X) = X^2 - X - t$.

Unterfall $p = 2$.

Unterunterfall $t \equiv_2 1$. Es ist $X^2 - X - \bar{t} \in \mathbf{F}_2[X]$ mangels Nullstelle in $\mathbf{F}_2$ irreduzibel. Wir erhalten die triviale Primidealfaktorzerlegung

$$(2) \;=\; 2\mathbf{Z}[\alpha] \;=\; (2)^1 \;.$$

Unterunterfall $t \equiv_2 0$. Es ist $X^2 - X - \bar{t} = X(X - 1) \in \mathbf{F}_2[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(2) \;=\; 2\mathbf{Z}[\alpha] \;=\; (2, \alpha)^1 (2, \alpha - 1)^1 \;.$$

Unterfall $p \neq 2$. Wähle ein $u \in \mathbf{Z}$ mit $2u \equiv_p 1$.

Unterunterfall $\bar{d} \in (\mathbf{F}_p^\times)^2$. Wähle ein $s \in \mathbf{Z}$ mit $s^2 \equiv_p d$. Es ist $X^2 - X - \bar{t} = (X - \bar{u} + \bar{u}\bar{s})(X - \bar{u} - \bar{u}\bar{s}) \in \mathbf{F}_p[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(p) \;=\; p\mathbf{Z}[\alpha] \;=\; (p, \alpha - u + us)^1 (p, \alpha - u - us)^1 \;.$$

Unterunterfall $\bar{d} \notin (\mathbf{F}_p^\times)^2$. Es ist $X^2 - X - \bar{t} \in \mathbf{F}_p[X]$ mangels Nullstelle irreduzibel. Denn *gäbe* es ein $x \in \mathbf{Z}$ mit $0 = \bar{x}^2 - \bar{x} - \bar{t} = (\bar{x} - \bar{u})^2 - (\bar{u}^2 + \bar{t})$, dann wäre $(\mathbf{F}_p^\times)^2 \ni 4(\bar{u}^2 + \bar{t}) = \bar{1} + 4\bar{t} = \bar{d}$, was *nicht* so ist. Wir erhalten die triviale Primidealfaktorzerlegung

$$(p) \;=\; p\mathbf{Z}[\alpha] \;=\; (p)^1 \;.$$

Ad (4). Schreibe $\delta := \sqrt[3]{2}$. Es ist $\mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$; cf. Aufgabe 19. Es ist $\mu_{\delta,\mathbf{Q}}(X) = X^3 - 2$.

Wir suchen die Primidealfaktorzerlegung von $(p) = p\mathbf{Z}[\delta]$ für $p \in \{2, 3, 5, 7\}$.

Fall $p = 2$. Es ist $X^3 - \bar{2} = X^3 \in \mathbf{F}_2[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(2) \;=\; 2\mathbf{Z}[\delta] \;=\; (2, \delta)^3 = (\delta)^3 \;.$$

Fall $p = 3$. Es ist $X^3 - \bar{2} = (X + \bar{1})^3 \in \mathbf{F}_3[X]$. Wir erhalten die Primidealfaktorzerlegung

$$(3) \;=\; 3\mathbf{Z}[\delta] \;=\; (3, \delta + 1)^3 \;=\; (\delta + 1)^3 \;,$$

beachte hierzu noch $3 = (\delta + 1)^3 - 3\delta(\delta + 1) \in (\delta + 1)$.

Fall $p = 5$. Es ist $X^3 - \bar{2} = (X + \bar{2})(X^2 - \bar{2}X - \bar{1}) \in \mathbf{F}_5[X]$, wobei der quadratische Faktor mangels Nullstelle irreduzibel ist. Wir erhalten die Primidealfaktorzerlegung

$$(5) \;=\; 5\mathbf{Z}[\delta] \;=\; (5, \delta + 2)^1 (5, \delta^2 - 2\delta - 1)^1 \;.$$

Beachte noch, daß als Elemente $(\delta^2-2\delta-1)(-\delta^2-1)=5$ ist und folglich als Ideale

$$(5,\delta^2-2\delta-1) \;=\; (\delta^2-2\delta-1)\;.$$

Also ist als Ideale auch $(5)=(\delta^2+1)(\delta^2-2\delta-1)$. Wegen der Eindeutigkeit der Primidealfaktorzerlegung folgt $(5,\delta+2)=(\delta^2+1)$. Folglich können wir unsere Primidealfaktorzerlegung auch schreiben als

$$(5) \;=\; 5\mathbf{Z}[\delta] \;=\; (\delta^2+1)^1(\delta^2-2\delta-1)^1\;.$$

Fall $p=7$. Es ist $X^3-\bar{2}\in\mathbf{F}_7[X]$ mangels Nullstelle irreduzibel. Wir erhalten die triviale Primidealfaktorzerlegung

$$(7) \;=\; 7\mathbf{Z}[\delta] \;=\; (7)^1\;.$$

Oft verzichtet man auch auf eine Kennzeichnung der Restklassen und schreibt mißbräuchlicherweise nur $2:=\bar{2}$ etc.

Aufgabe 31

Sei $x\in B_{\mathfrak{p}}$. Zu zeigen ist $x\overset{!}{\in}A_{\mathfrak{p}}[b]$.

Schreibe $x=s^{-1}\tilde{b}$ mit $\tilde{b}\in B$ und $s\in A\smallsetminus\mathfrak{p}$. Da $B=A[b]$, gibt es $k\geqslant 0$ und $a_i\in A$ für $i\in[0,k]$ mit $\tilde{b}=a_kb^k+\cdots+a_0b^0$. Folglich ist

$$x \;=\; s^{-1}\tilde{b} \;=\; s^{-1}(a_kb^k+\cdots+a_0b^0) \;=\; s^{-1}a_kb^k+\cdots+s^{-1}a_0b^0 \;\in\; A_{\mathfrak{p}}[b]\;.$$

Aufgabe 32

Sei $S=\mathbf{Z}\smallsetminus((2)\cup(3))$. Es ist $1\in S$. Für $s,\,t\in S$, i.e. s und t teilerfremd zu 6, ist auch st teilerfremd zu 6, i.e. $st\in S$.

Gemäß Lemma 70.(3) ist auch $A:=S^{-1}\mathbf{Z}$ ein Hauptidealbereich.

Gemäß Aufgabe 10.(1) ist $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(S^{-1}\mathbf{Z})$ in Bijektion mit $\{\,\mathfrak{p}\in\mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z})\,:\,\mathfrak{p}\cap S=\emptyset\,\}$. Ist $p\in\mathbf{Z}_{>0}$ eine Primzahl mit $p\notin\{2,3\}$, dann ist $p\in(p)\cap S$ und somit $(p)\cap S\neq\emptyset$. Dagegen ist $(2)\cap S=\emptyset$ und $(3)\cap S=\emptyset$. Also ist $|\,\mathrm{Ideale}^{\times}_{\mathrm{prim}}(S^{-1}\mathbf{Z})|=2$. Genauer, es ist $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(S^{-1}\mathbf{Z})=\{(2),(3)\}$, gelesen als Ideale in $S^{-1}\mathbf{Z}$.

Aufgabe 33

Vorbemerkung. Wir können $t\in D^{\times}$ und $\mathfrak{a},\,\mathfrak{b}\,\in\,\mathrm{Ideale}^{\times}(D)$ wählen mit $\mathfrak{g}=\frac{1}{t}\mathfrak{a}$ und $\mathfrak{h}=\frac{1}{t}\mathfrak{b}$. Denn ist $\mathfrak{g}=\frac{d'}{t'}\mathfrak{a}_0$ und $\mathfrak{h}=\frac{d''}{t''}\mathfrak{b}_0$ mit d', d'', t', $t''\,\in\,D^{\times}$ und setzen wir $t:=t't''$, $\mathfrak{a}:=d't''\mathfrak{a}_0$, $\mathfrak{b}:=d''t'\mathfrak{b}_0$, dann wird $\mathfrak{g}=\frac{1}{t't''}d't''\mathfrak{a}_0=\frac{1}{t}\mathfrak{a}$ und $\mathfrak{h}=\frac{1}{t't''}d''t'\mathfrak{b}_0=\frac{1}{t}\mathfrak{b}$.

Ad (1). Es ist $S^{-1}\mathfrak{a}\in\mathrm{Ideale}^{\times}(S^{-1}D)$; cf. Aufgabe 10.(1). Es ist $\frac{1}{t}\in\mathrm{Quot}(S^{-1}D)^{\times}=\mathrm{Quot}(D)^{\times}$. Also ist $S^{-1}\mathfrak{g}=\frac{1}{t}S^{-1}\mathfrak{a}\in\underline{\mathrm{Ideale}}^{\times}_{\mathrm{prim}}(S^{-1}D)$.

Ad (2). Es ist $S^{-1}(\mathfrak{gh})\;=\;S^{-1}(\frac{1}{t^2}\mathfrak{ab})x\;=\;\frac{1}{t^2}S^{-1}(\mathfrak{ab})\;=\;\frac{1}{t^2}(S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})\;=\;(S^{-1}\frac{1}{t}\mathfrak{a})(S^{-1}\frac{1}{t}\mathfrak{b})\;=\;(S^{-1}\mathfrak{g})(S^{-1}\mathfrak{h})$; cf. Aufgabe 29.(8). Wegen $(S^{-1}(\mathfrak{g}^{-1}))(S^{-1}\mathfrak{g})\;=\;S^{-1}(\mathfrak{g}^{-1}\mathfrak{g})\;=\;S^{-1}D$ ist $S^{-1}(\mathfrak{g}^{-1})\;=\;(S^{-1}\mathfrak{g})^{-1}$.

Ad (3). Es ist $S^{-1}(\mathfrak{g}+\mathfrak{h})\;=\;S^{-1}(\frac{1}{t}\mathfrak{a}+\frac{1}{t}\mathfrak{b})\;=\;S^{-1}(\frac{1}{t}(\mathfrak{a}+\mathfrak{b}))\;=\;\frac{1}{t}S^{-1}(\mathfrak{a}+\mathfrak{b})\;=\;\frac{1}{t}(S^{-1}\mathfrak{a}+S^{-1}\mathfrak{b})\;=\;\frac{1}{t}S^{-1}\mathfrak{a}+\frac{1}{t}S^{-1}\mathfrak{b}=S^{-1}\frac{1}{t}\mathfrak{a}+S^{-1}\frac{1}{t}\mathfrak{b}=S^{-1}\mathfrak{g}+S^{-1}\mathfrak{h}$; cf. Aufgabe 29.(8).

Es ist $S^{-1}(\mathfrak{g}\cap\mathfrak{h})=S^{-1}(\frac{1}{t}\mathfrak{a}\cap\frac{1}{t}\mathfrak{b})=S^{-1}(\frac{1}{t}(\mathfrak{a}\cap\mathfrak{b}))=\frac{1}{t}S^{-1}(\mathfrak{a}\cap\mathfrak{b})=\frac{1}{t}(S^{-1}\mathfrak{a}\cap S^{-1}\mathfrak{b})=\frac{1}{t}S^{-1}\mathfrak{a}\cap\frac{1}{t}S^{-1}\mathfrak{b}=S^{-1}\frac{1}{t}\mathfrak{a}\cap S^{-1}\frac{1}{t}\mathfrak{b}=S^{-1}\mathfrak{g}\cap S^{-1}\mathfrak{h}$; cf. Aufgabe 29.(8).

Ad (4). Es ist $\mathrm{v}_\mathfrak{p}(\mathfrak{g}) = \mathrm{v}_\mathfrak{p}(\frac{1}{t}\mathfrak{a}) = -\mathrm{v}_\mathfrak{p}(t) + \mathrm{v}_\mathfrak{p}(\mathfrak{a})$; cf. Lemma 65. Es wird $\mathfrak{g}_\mathfrak{p} = (\frac{1}{t}\mathfrak{a})_\mathfrak{p} = ((t)^{-1}\mathfrak{a})_\mathfrak{p} = ((t)_\mathfrak{p})^{-1}\mathfrak{a}_\mathfrak{p} = ((\mathfrak{p}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}((t))})^{-1}(\mathfrak{p}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}(\mathfrak{a})} = (\mathfrak{p}_\mathfrak{p})^{-\mathrm{v}_\mathfrak{p}(t)+\mathrm{v}_\mathfrak{p}(\mathfrak{a})} = (\mathfrak{p}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}(\mathfrak{g})}$; cf. Aufgabe 29.(8).

Ad (5). Es ist $\mathfrak{g} = \frac{1}{t}\mathfrak{a} \overset{\text{L. 77}}{=} \frac{1}{t}\bigcap_{\mathfrak{p}\in\mathrm{Ideale}^\times_{\mathrm{prim}}(D)} \mathfrak{a}_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\mathrm{Ideale}^\times_{\mathrm{prim}}(D)} \frac{1}{t}\mathfrak{a}_\mathfrak{p} \overset{\text{D. 80}}{=} \bigcap_{\mathfrak{p}\in\mathrm{Ideale}^\times_{\mathrm{prim}}(D)} \mathfrak{g}_\mathfrak{p}$.

Aufgabe 34

Ad (1). Es ist $\mathrm{N}_{L|K}(\mathfrak{g}^{-1})\,\mathrm{N}_{L|K}(\mathfrak{g}) \overset{\text{L. 88}}{=} \mathrm{N}_{L|K}(\mathfrak{g}^{-1}\mathfrak{g}) = \mathrm{N}_{L|K}((1)) \overset{\text{B. 86.(3)}}{=} (\mathrm{N}_{L|K}(1)) = (1)$. Also ist $\mathrm{N}_{L|K}(\mathfrak{g}^{-1}) = \mathrm{N}_{L|K}(\mathfrak{g})^{-1}$.

Ad (2). Es genügt, $\mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\mathfrak{h}))_\mathfrak{p} \overset{!}{=} \mathrm{N}_{M|K}(\mathfrak{h})_\mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ zu zeigen; cf. Bemerkung 81.(5). Dank Lemma 87 bedeutet dies $\mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\mathfrak{h}_\mathfrak{p})) \overset{!}{=} \mathrm{N}_{M|K}(\mathfrak{h}_\mathfrak{p})$. Nun sind $A_\mathfrak{p}$, $B_\mathfrak{p}$ und $C_\mathfrak{p}$ Hauptidealbereiche, es ist $K = \mathrm{Quot}(A_\mathfrak{p})$, $L = \mathrm{Quot}(B_\mathfrak{p})$, $M = \mathrm{Quot}(C_\mathfrak{p})$, und es ist $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$, $C_\mathfrak{p} = \Gamma_M(A_\mathfrak{p})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A, B und C als Hauptidealbereiche voraussetzen. Ist nun $\mathfrak{h} = (h)$ mit $h \in M^\times$, dann wird in der Tat

$$\mathrm{N}_{L|K}(\mathrm{N}_{M|L}((h))) \overset{\text{B. 86.(3)}}{=} (\mathrm{N}_{L|K}(\mathrm{N}_{M|L}(h))) \overset{\text{L. 19.(2)}}{=} (\mathrm{N}_{M|K}(h)) \overset{\text{B. 86.(3)}}{=} \mathrm{N}_{M|K}((h)) .$$

Ad (3). Es genügt, $\mathrm{N}_{L|K}(\mathfrak{f}B)_\mathfrak{p} \overset{!}{=} (\mathfrak{f}^\ell)_\mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ zu zeigen; cf. Bemerkung 81.(5).

Dank Lemma 87 und Bemerkung 81.(2) bedeutet dies $\mathrm{N}_{L|K}(\mathfrak{f}_\mathfrak{p}B_\mathfrak{p}) \overset{!}{=} (\mathfrak{f}_\mathfrak{p})^\ell$. Nun sind $A_\mathfrak{p}$ und $B_\mathfrak{p}$ Hauptidealbereiche und es ist $K = \mathrm{Quot}(A_\mathfrak{p})$ sowie $L = \mathrm{Quot}(B_\mathfrak{p})$, und es ist $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Ist nun $\mathfrak{f} = (f)$ mit $f \in K^\times$, dann wird in der Tat

$$\mathrm{N}_{L|K}((f)B) = \mathrm{N}_{L|K}((f)) \overset{\text{B. 86.(3)}}{=} (\mathrm{N}_{L|K}(f)) \overset{\text{L. 15.(2)}}{=} (f^\ell) = (f)^\ell .$$

Aufgabe 35

Ad (1). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Es ist $\mathbf{Z}[\mathrm{i}]^\# = {}_\mathbf{Z}\langle \frac{1}{2} \rangle \oplus {}_\mathbf{Z}\langle \frac{1}{2}\mathrm{i} \rangle$; cf. Beispiel 32.(1).

Für $a, b \in \mathbf{Q}$ ist dagegen $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(a + b\mathrm{i}) = 2a$ genau dann in $\mathbf{Z}$, wenn $a + b\mathrm{i} \in {}_\mathbf{Z}\langle \frac{1}{2} \rangle \oplus {}_\mathbf{Q}\langle \mathrm{i} \rangle$ liegt.

Also ist hier $\mathbf{Z}[\mathrm{i}]^\#$ im Urbild von $\mathbf{Z}$ unter $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}$ echt enthalten.

Ad (2). Die Aussage ist richtig.

Zeigen wir $(B^\#)_\mathfrak{p} \overset{!}{\subseteq} (B_\mathfrak{p})^\#$. Dazu genügt $B^\# \overset{!}{\subseteq} (B_\mathfrak{p})^\#$. Ist aber $y \in L$ gegeben mit $\mathrm{Tr}_{L|K}(yB) \subseteq A$, dann ist auch $\mathrm{Tr}_{L|K}(yB_\mathfrak{p}) \subseteq A_\mathfrak{p}$, da für $b \in B$ und $s \in A \setminus \mathfrak{p}$ sich dann $\mathrm{Tr}_{L|K}(y\frac{b}{s}) = \frac{1}{s}\mathrm{Tr}_{L|K}(yb) \in A_\mathfrak{p}$ ergibt.

Zeigen wir $(B^\#)_\mathfrak{p} \overset{!}{\supseteq} (B_\mathfrak{p})^\#$. Sei $y \in K$ gegeben mit $\mathrm{Tr}_{L|K}(yB_\mathfrak{p}) \subseteq A_\mathfrak{p}$. Wir haben zu zeigen, daß es ein $s \in A \setminus \mathfrak{p}$ gibt mit $sy \in B^\#$, i.e. mit $\mathrm{Tr}_{L|K}(syB) \subseteq A$.

Dank Aufgabe 24.(5) ist B ein endlich erzeugter A-Modul. Schreibe demgemäß $B = {}_A\langle b_1, \ldots, b_m \rangle$ mit $m \geqslant 0$ und $b_i \in B$ für $i \in [1, m]$. Schreibe $\mathrm{Tr}_{L|K}(yb_i) = \frac{a_i}{s}$ mit $s \in A \setminus \mathfrak{p}$ und $a_i \in A$ für $i \in [1, m]$. Es ist $\mathrm{Tr}_{L|K}(syb_i) = a_i \in A$ für $i \in [1, m]$. Also ist $\mathrm{Tr}_{L|K}(syB) \subseteq A$.

Ad (3). Die Aussage ist falsch.

Sei $K := \mathbf{Q}$, $L := \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.. Sei $x := 2 + \mathrm{i}$ und $y := 2 - \mathrm{i}$. Dann ist

$$\mathrm{N}_{L|K}(\,(x,y)\,) \;\ni\; 16 \;=\; \mathrm{N}_{L|K}(x+y) \;=\; \mathrm{N}_{L|K}(4) \;=\; 16\,,$$

aber

$$(\,\mathrm{N}_{L|K}(x),\,\mathrm{N}_{L|K}(y)\,) \;=\; (\,5,\,5\,) \;=\; (5) \;\not\ni\; 16\,.$$

Ad (4). Die Aussage ist richtig.

Sei E ein Zerfällungskörper von $L|K$. Sei $G := \mathrm{Gal}(L|K)$. Sei $U := \mathrm{Gal}(E|L)$. Sei $G = \bigsqcup_{i\in[1,\ell]} \sigma_i U$, wobei $\ell := [L:K]$ und $\sigma_i \in G$ für $i \in [1,\ell]$. Hierbei sei o.E. $\sigma_1 = \mathrm{id}_E$.

Sei $b \in \mathfrak{b}^\times$. Schreibe $b' := \prod_{i\in[2,\ell]} \sigma_i(b)$. Es ist $\mathrm{N}_{L|K}(b) \overset{\text{L. 15}}{=} bb'$. Folglich ist $b' = \frac{\mathrm{N}_{L|K}(b)}{b} \in L$. Es ist aber auch $b' = \prod_{i\in[2,\ell]} \sigma_i(b) \in \Gamma_E(A)$; cf. Lemma 20.(1). Zusammen ist $b' \in L \cap \Gamma_E(A) = \Gamma_L(A) = B$. Also ist $\mathrm{N}_{L|K}(b) = bb' \in \mathfrak{b}$. Insgesamt ist $\mathrm{N}_{L|K}(b) \in A \cap \mathfrak{b}$; cf. Lemma 20.(3).

Cf. auch Beweis zu Lemma 120.

Ad (5). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Sei $\mathfrak{b} := (2) \in \mathrm{Ideale}^\times(\mathbf{Z}[\mathrm{i}])$.

Es ist $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(2)\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(2)\,) = (4)$.

Es ist $(2) \cap \mathbf{Z} = (2)$.

Also ist in diesem Fall $\mathrm{N}_{L|K}(\mathfrak{b}) \subset \mathfrak{b} \cap A$.

Ad (6). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Es ist $(2+\mathrm{i}) \neq (2-\mathrm{i})$, da $\frac{2+\mathrm{i}}{2-\mathrm{i}} = \frac{1}{5}(3+4\mathrm{i}) \notin \mathbf{Z}[\mathrm{i}]$.

Dahingegen ist $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(2+\mathrm{i})\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(2+\mathrm{i})\,) = (5)$ und $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(2-\mathrm{i})\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(2-\mathrm{i})\,) = (5)$.

Ad (7). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Wir behaupten, daß $(3) \in \underline{\mathrm{Ideale}}^\times(\mathbf{Z})$ nicht im Bild von $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}$ liegt. *Annahme,* doch. Sei $\mathfrak{g} \in \underline{\mathrm{Ideale}}^\times(\mathbf{Z}[\mathrm{i}])$ mit $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\mathfrak{g}) = (3)$.

Da $\mathbf{Z}[\mathrm{i}]$ ein Hauptidealbereich ist, können wir $\mathfrak{g} = (a+b\mathrm{i})$ schreiben, mit $a, b \in \mathbf{Q}$; cf. Aufgabe 6.(2). Gemäß Bemerkung 86.(3) ist also $(\,\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(a+b\mathrm{i})\,) = (3)$, i.e. $a^2 + b^2 \in \{-3, +3\}$, i.e. $a^2 + b^2 = 3$. Schreibe $a = \frac{u}{s}$ und $b = \frac{v}{s}$, mit $u, v \in \mathbf{Z}$ und $s \in \mathbf{Z}^\times$ derart, daß es keine Primzahl gibt, die a, b und s teilt. Dann ist $u^2 + v^2 = 3s^2$. Folglich ist $u^2 + v^2 \equiv_3 0$. Da in $\mathbf{F}_3$ nur die Quadrate 0 und 1 liegen, erzwingt dies $u \equiv_3 0$ und $v \equiv_3 0$. Dann aber ist $0 \equiv_9 u^2 + v^2 = 3s^2$, und somit $0 \equiv_3 s$. *Widerspruch.*

Ad (8). Die Aussage ist richtig.

Wir benötigen folgende allgemeine Aussage, die eine Variante von Lemma 77 darstellt.

Sei $\tilde{\mathfrak{b}} \in \mathrm{Ideale}^\times(B)$. Wir *behaupten* $\tilde{\mathfrak{b}} = \bigcap_{\mathfrak{p}\in\mathrm{Ideale}^\times_{\mathrm{prim}}(A)} \tilde{\mathfrak{b}}_{\mathfrak{p}}$. Sei $x \in L$ in der rechten Seite enthalten. Wir haben $x \overset{!}{\in} B$ zu zeigen. Sei $\mathfrak{a} := \{\, a \in A : ax \in \mathfrak{b} \,\}$. Es ist $\mathfrak{a} \in \mathrm{Ideale}(A)$. Wir haben $1 \in \mathfrak{a}$ zu zeigen. Es genügt zu zeigen, daß es für alle $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ ein $s \in A \smallsetminus \mathfrak{p}$ gibt, da dann $\mathfrak{a}$ in keinem maximalen Ideal enthalten ist und also $\mathfrak{a} = A$ folgt; cf. Bemerkung 51.(4). Aber es ist $x \in \tilde{\mathfrak{b}}_{\mathfrak{p}}$ und also $x = \frac{b}{s}$ für ein $b \in \mathfrak{b}$ und ein $s \in A \smallsetminus \mathfrak{p}$, was $sx \in \mathfrak{b}$ nach sich zieht. Dies zeigt die *Behauptung.*

Es genügt, $(\mathrm{N}_{L|K}(\mathfrak{b})B)_\mathfrak{p} \stackrel{!}{=} (\prod_{\sigma\in G}\sigma(\mathfrak{b}))_\mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ zu zeigen; cf. Behauptung.

Dank Lemma 87 und Aufgabe 29.(8) bedeutet dies $\mathrm{N}_{L|K}(\mathfrak{b}_\mathfrak{p})B_\mathfrak{p} \stackrel{!}{=} \prod_{\sigma\in G}\sigma(\mathfrak{b}_\mathfrak{p})$. Nun sind $A_\mathfrak{p}$ und $B_\mathfrak{p}$ Hauptidealbereiche und es ist $K = \mathrm{Quot}(A_\mathfrak{p})$ sowie $L = \mathrm{Quot}(B_\mathfrak{p})$, und es ist $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Ist nun $\mathfrak{b} = (b)$ mit $b \in B^\times$, dann wird in der Tat

$$\mathrm{N}_{L|K}(\,(b)\,)B \stackrel{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{L|K}(b)\,)B \;=\; (\,\mathrm{N}_{L|K}(b)\,) \stackrel{\text{B. 16.(2)}}{=} (\,\prod_{\sigma\in G}\sigma(b)\,) \;=\; \prod_{\sigma\in G}\sigma(\,(b)\,)\,.$$

Ad (9). Die Aussage ist richtig.

Es genügt, $((B\mathfrak{a})\cap A)_\mathfrak{p} \stackrel{!}{=} \mathfrak{a}_\mathfrak{p}$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$ zu zeigen; cf. Lemma 77.

Dank Aufgabe 29.(8) bedeutet dies $(B_\mathfrak{p}\mathfrak{a}_\mathfrak{p})\cap A_\mathfrak{p} \stackrel{!}{=} \mathfrak{a}_\mathfrak{p}$. Nun sind $A_\mathfrak{p}$ und $B_\mathfrak{p}$ Hauptidealbereiche und es ist $K = \mathrm{Quot}(A_\mathfrak{p})$ sowie $L = \mathrm{Quot}(B_\mathfrak{p})$, und es ist $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Ist nun $\mathfrak{a} = (a)$ mit $a \in A^\times$, dann haben wir $B(a)\cap A \stackrel{!}{=} (a)$ zu zeigen. Dabei ist nur $B(a)\cap A \stackrel{!}{\subseteq} (a)$ zu zeigen. Sei also $b \in B^\times$ und $a \in A^\times$ gegeben mit $ba \in A$. Es genügt, $b \stackrel{!}{\in} A$ zu zeigen. Es ist $b = \frac{ba}{a} \in K$. Also ist $b \in B\cap K = \Gamma_L(A)\cap K = \Gamma_K(A) = A$; cf. Definition 52.

> Der Versuch, es direkt, also ohne Lokalisierung, zu zeigen, führt wegen der Tatsache, daß $B\mathfrak{a}$ aus Elementen der Form $\sum_i b_i a_i$ mit $b_i \in B$ und $a_i \in \mathfrak{a}$ besteht, wohl zu Problemen.

Ad (10). Die Aussage ist falsch.

Sei $K := \mathbf{Q}$, $L := \mathbf{Q}(\mathrm{i})$, $A := \mathbf{Z}$, $B := \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Sei $\mathfrak{g} := \mathbf{Z}[\mathrm{i}] = (1)$.

Es ist $\mathrm{N}_{L|K}(\mathfrak{g}) = \mathrm{N}_{L|K}(\,(1)\,) \stackrel{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{L|K}(1)\,) = (1) = \mathbf{Z}$.

Dagegen ist $\{\,\mathrm{N}_{L|K}(g) \,:\, g \in \mathfrak{g}\,\} = \{\,\mathrm{N}_{L|K}(a+b\mathrm{i}) \,:\, a,\, b \in \mathbf{Z}\,\} = \{\,a^2+b^2 \,:\, a,\, b \in \mathbf{Z}\,\}$.

Es ist e.g. 3 in ersterer Menge, nicht aber in letzterer enthalten. Somit ist hier

$$\mathrm{N}_{L|K}(\mathfrak{g}) \;\supset\; \{\,\mathrm{N}_{L|K}(g) \,:\, g \in \mathfrak{g}\,\}\,.$$

Ad (11). Die Aussage ist falsch.

Sei $K := \mathbf{Q}$. Sei $A := \mathbf{Z}$. Sei $L := \mathbf{Q}(\mathrm{i})$. Es ist $B = \Gamma_L(A) = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Sei $y := \frac{1}{5}(3+4\mathrm{i})$. Es ist $\mathrm{N}_{L|K}(y) = \frac{1}{5}(3+4\mathrm{i})\cdot\frac{1}{5}(3-4\mathrm{i}) = 1 \in \mathrm{U}(A)$; Cf. Aufgabe 12.

Sei $\mathfrak{g} = (y)$. Es ist $\mathfrak{g} \neq (1)$, da $y \notin B$. Aber es ist $\mathrm{N}_{L|K}(\mathfrak{g}) = \mathrm{N}_{L|K}(\,(y)\,) = (\,\mathrm{N}_{L|K}(y)\,) = (1)$; cf. Bemerkung 86.(3).

> Cf. Aufgabe 12.

Ad (12). Die Aussage ist richtig.

Ist $\mathfrak{b} = (1)$, dann ist $\mathrm{N}_{L|K}(\mathfrak{b}) = \mathrm{N}_{L|K}(\,(1)\,) = (\,\mathrm{N}_{L|K}(1)\,) = (1)$; cf. Bemerkung 86.(3).

Sei umgekehrt $\mathrm{N}_{L|K}(\mathfrak{b}) = (1)$. Insbesondere ist $\mathfrak{b} \neq (0)$. Wir haben $\mathfrak{b} \stackrel{!}{=} (1)$ zu zeigen. Es genügt, $\mathfrak{b}_\mathfrak{p} \stackrel{!}{=} (1)$ zu zeigen für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(A)$. Es ist $\mathrm{N}_{L|K}(\mathfrak{b}_\mathfrak{p}) = \mathrm{N}_{L|K}(\mathfrak{b})_\mathfrak{p} = (1)$; cf. Lemma 87. Nun sind $A_\mathfrak{p}$ und

$B_\mathfrak{p}$ Hauptidealbereiche und es ist $K = \mathrm{Quot}(A_\mathfrak{p})$ sowie $L = \mathrm{Quot}(B_\mathfrak{p})$, und es ist $B_\mathfrak{p} = \Gamma_L(A_\mathfrak{p})$; cf. Bemerkung 82.(1, 2, 3).

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Sei $\mathfrak{b} = (b)$ mit $b \in B^\times$. Es ist $(1) = \mathrm{N}_{L|K}(\mathfrak{b}) = \mathrm{N}_{L|K}(\,(b)\,) = (\,\mathrm{N}_{L|K}(b)\,)$; cf. Bemerkung 86.(3). Also ist $\mathrm{N}_{L|K}(b) \in \mathrm{U}(A)$; cf. Bemerkung 66.(3). Somit ist $b \in \mathrm{U}(B)$; cf. Lemma 20.

Aufgabe 36

Ad (1). Schreibe $\alpha := \frac{1}{2}(1 + \sqrt{-23})$. Beachte $\alpha^2 = \alpha - 6$. Es ist $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-23})$.

Es ist $\mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha] = {}_\mathbf{Z}\langle 1, \alpha\rangle$; cf. Aufgabe 3.

Schreibe $\mathfrak{p} := (2, \alpha)$.

> Gemäß Lösung zu Aufgabe 30.(3) ist $\mathfrak{p}$ übrigens ein Primideal.

Es ist $\mathfrak{p} = {}_\mathbf{Z}\langle 2, 2\alpha, \alpha, \alpha^2\rangle = {}_\mathbf{Z}\langle 2, \alpha, \alpha - 6\rangle = {}_\mathbf{Z}\langle 2, \alpha\rangle$. Also ist $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}) = (\det \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = (2)$; cf. Lemma 90.

Annahme, es ist $\mathfrak{p}$ ein Hauptideal. Dann ist $\mathfrak{p} = (u + v\alpha)$ für gewisse $u, v \in \mathbf{Z}$ und also $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}) = \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\,(u + v\alpha)\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(u + v\alpha)\,) = (\det \left(\begin{smallmatrix} u & -6v \\ v & u+v \end{smallmatrix}\right)) = (u^2 + uv + 6v^2) = ((u + \frac{1}{2}v)^2 + \frac{23}{4}v^2)$. Es folgt $(u + \frac{1}{2}v)^2 + \frac{23}{4}v^2 = 2$, i.e. $(2u + v)^2 + 23v^2 = 8$, was zu $v = 0$ und $u^2 = 2$ führt. Wir haben einen *Widerspruch.*

Es bleibt zu zeigen, daß $\mathfrak{p}^3$ ein Hauptideal ist. Denn dann ist die Ordnung von $[\mathfrak{p}]$, von der wir schon wissen, daß sie nicht 1 ist, ein Teiler von 3 und somit gleich 3.

Es ist $\mathfrak{p}^3 = (8, 4\alpha, 2\alpha^2, \alpha^3) = (8, 4\alpha, 2\alpha - 12, -5\alpha - 6) = (8, 4\alpha, 2\alpha - 12, -\alpha + 2) = (8, 4\alpha, 2 - \alpha) = (8, 2 - \alpha)$.

Wir behaupten, daß $\mathfrak{p}^3 \overset{!}{=} (2 - \alpha)$ ist. In der Tat ist $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(2 - \alpha) = 2^2 + 2 \cdot (-1) + 6(-1)^2 = 8$ ein $\mathbf{Z}[\alpha]$-Vielfaches von $2 - \alpha$; cf. Lemma 15.(2).

> Alternativ hätte man auch mittels $(2 - \alpha) \subseteq \mathfrak{p}$ und $(|\mathcal{O}_{\mathbf{Q}(\alpha)|\mathbf{Q}}/\mathfrak{p}^5|) = \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}^3) = (\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\alpha - 2)) = (|\mathcal{O}_{\mathbf{Q}(\alpha)|\mathbf{Q}}/(2 - \alpha)|)$ verwenden können, um auf $\mathfrak{p}^3 \overset{!}{=} (2 - \alpha)$ zu schließen; cf. Lemma 91, Bemerkung 86.(3).

Ad (2). Schreibe $\alpha := \frac{1}{2}1 + \sqrt{-47}$. Beachte $\alpha^2 = \alpha - 12$. Es ist $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-47})$.

Es ist $\mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha] = {}_\mathbf{Z}\langle 1, \alpha\rangle$; cf. Aufgabe 3.

Schreibe $\mathfrak{p} := (2, \alpha)$.

> Gemäß Lösung zu Aufgabe 30.(3) ist $\mathfrak{p}$ übrigens ein Primideal.

Es ist $\mathfrak{p} = {}_\mathbf{Z}\langle 2, 2\alpha, \alpha, \alpha^2\rangle = {}_\mathbf{Z}\langle 2, \alpha, \alpha - 12\rangle = {}_\mathbf{Z}\langle 2, \alpha\rangle$. Also ist $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}) = (\det \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = (2)$; cf. Lemma 90.

Annahme, es ist $\mathfrak{p}$ ein Hauptideal. Dann ist $\mathfrak{p} = (u + v\alpha)$ für gewisse $u, v \in \mathbf{Z}$ und also $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}) = \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\,(u + v\alpha)\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(u + v\alpha)\,) = (\det \left(\begin{smallmatrix} u & -12v \\ v & u+v \end{smallmatrix}\right)) = (u^2 + uv + 12v^2) = ((u + \frac{1}{2}v)^2 + \frac{47}{4}v^2)$. Es folgt $(u + \frac{1}{2}v)^2 + \frac{47}{4}v^2 = 2$, i.e. $(2u + v)^2 + 47v^2 = 8$, was zu $v = 0$ und $u^2 = 2$ führt. Wir haben einen *Widerspruch.*

Es bleibt zu zeigen, daß $\mathfrak{p}^5$ ein Hauptideal ist. Denn dann ist die Ordnung von $[\mathfrak{p}]$, von der wir schon wissen, daß sie nicht 1 ist, ein Teiler von 5 und somit gleich 5.

Es ist $\mathfrak{p}^5 = (32, 16\alpha, 8\alpha^2, 4\alpha^3, 2\alpha^4, \alpha^5) = (32, 16\alpha, 8\alpha - 96, -44\alpha - 48, -46\alpha + 264, 109\alpha + 276) = (32, 16\alpha, 8\alpha, 4\alpha + 16, 2\alpha + 8, -3\alpha - 12) = (32, 8\alpha, 2\alpha + 8, -\alpha - 4) = (32, 8\alpha, 4 + \alpha) = (32, 4 + \alpha)$.

Wir behaupten, daß $\mathfrak{p}^5 \stackrel{!}{=} (4+\alpha)$ ist. In der Tat ist $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(4+\alpha) = 4^2 + 4\cdot 1 + 12\cdot 1^2 = 32$ ein $\mathbf{Z}[\alpha]$-Vielfaches von $4+\alpha$; cf. Lemma 15.(2).

Alternativ hätte man auch mittels $(4+\alpha) \subseteq \mathfrak{p}$ und $(|\mathcal{O}_{\mathbf{Q}(\alpha)|\mathbf{Q}}/\mathfrak{p}^5|) = \mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(\mathfrak{p}^5) = (\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(4+\alpha)) = (|\mathcal{O}_{\mathbf{Q}(\alpha)|\mathbf{Q}}/(4+\alpha)|)$ verwenden können, um auf $\mathfrak{p}^5 \stackrel{!}{=} (4+\alpha)$ zu schließen; cf. Lemma 91, Bemerkung 86.(3).

Aufgabe 37

Ad (1). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Sei $\mathfrak{b} := (1+\mathrm{i}) \in \mathrm{Ideale}^\times(\mathbf{Z}[\mathrm{i}])$.

Es ist $\mathfrak{b} \cap A = (1+\mathrm{i}) \cap \mathbf{Z} = (2)$. Denn $2 = (1-\mathrm{i})(1+\mathrm{i}) \in (1+\mathrm{i})$, und also $(2) \subseteq (1+\mathrm{i}) \cap \mathbf{Z}$. Es ist $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(1+\mathrm{i}) = 2$, also $(1+\mathrm{i}) \subset \mathbf{Z}[\mathrm{i}]$, also $1 \notin (1+\mathrm{i})$, also $(1+\mathrm{i}) \cap \mathbf{Z} \subset \mathbf{Z}$. Da $(2) \subset \mathbf{Z}$ maximal ist, folgt $(2) = (1+\mathrm{i}) \cap \mathbf{Z}$.

Nun ist $B(\mathfrak{b} \cap A) = \mathbf{Z}[\mathrm{i}](2) = (2)$. Aber $\mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(1+\mathrm{i})\,) = (2) \neq (4) = \mathrm{N}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(2)\,) = (4)$, sodaß $\mathfrak{b} \neq B(\mathfrak{b} \cap A)$ ist.

Ad (2). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3. Sei $\mathfrak{b} := (1+\mathrm{i})$ und $\mathfrak{b}' = (1-\mathrm{i})$ in $\mathrm{Ideale}^\times(\mathbf{Z}[\mathrm{i}])$.

Es ist $A \cap \mathfrak{b} = (2)$; cf. Lösung zu (1). Sei $\sigma : \mathbf{Q}(\mathrm{i}) \stackrel{\sim}{\to} \mathbf{Q}(\mathrm{i})$, $\mathrm{i} \mapsto -\mathrm{i}$. Es ist $\mathfrak{b}' = \sigma(\mathfrak{b})$ und also $A \cap \mathfrak{b}' = A \cap \sigma(\mathfrak{b}) = \sigma(A \cap \mathfrak{b}) = \sigma(\,(2)\,) = (2)$. Also ist $(A \cap \mathfrak{b})(A \cap \mathfrak{b}') = (4)$. Auf der anderen Seite ist $A \cap (\mathfrak{b}\mathfrak{b}') = A \cap (\,(1-\mathrm{i})(1+\mathrm{i})\,) = A \cap (2) = (2)$, letzteres, da $2 \in A \cap (2)$ und $1 \notin A \cap (2)$.

Ad (3). Die Aussage ist richtig.

Es ist $\mathrm{Tr}_{L|K}(\mathfrak{b})$ ein Ideal in A. Denn es ist $0 = \mathrm{Tr}_{L|K}(0) \in \mathrm{Tr}_{L|K}(\mathfrak{b})$. Und sind b, $b' \in \mathfrak{b}$ und a, $a' \in A$, dann ist $a\,\mathrm{Tr}_{L|K}(b) + a'\,\mathrm{Tr}_{L|K}(b') = \mathrm{Tr}_{L|K}(ab + a'b') \in \mathrm{Tr}_{L|K}(\mathfrak{b})$.

Wähle $x \in L$ mit $\mathrm{Tr}_{L|K}(x) \neq 0$; cf. Lemma 18. Es ist $x \neq 0$. Sei $a \in A^\times$ mit $ax \in B^\times$; cf. Lemma 27.

Sei $b \in \mathfrak{b}^\times$. Sei $a' \in A^\times$ mit $a'b^{-1} \in B^\times$; cf. Lemma 27. Es ist $a' = (a'b^{-1})b \in \mathfrak{b}^\times$. Also ist $a'ax \in \mathfrak{b}$. Es wird $\mathrm{Tr}_{L|K}(\mathfrak{b}) \ni \mathrm{Tr}_{L|K}(a'ax) = a'a\,\mathrm{Tr}_{L|K}(x) \neq 0$.

Ad (4). Die Aussage ist richtig.

Schreibe $\mathfrak{h} = t^{-1}\mathfrak{b}$ mit $t \in A^\times$ und $\mathfrak{b} \in \mathrm{Ideale}^\times(B)$; cf. Lemma 88. Dann ist $\mathrm{Tr}_{L|K}(\mathfrak{h}) = \mathrm{Tr}_{L|K}(t^{-1}\mathfrak{b}) = t^{-1}\,\mathrm{Tr}_{L|K}(\mathfrak{b}) \in \underline{\mathrm{Ideale}}^\times(A)$ nach (3).

Ad (5). Die Aussage ist falsch.

Sei $K = \mathbf{Q}$, $L = \mathbf{Q}(\mathrm{i})$, $A = \mathbf{Z}$, $B = \mathbf{Z}[\mathrm{i}]$; cf. Aufgabe 3.

Es ist $\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(\,(2+\mathrm{i})\,) = \{\,\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}((2+\mathrm{i})(u+v\mathrm{i})) \,:\, u,\, v \in \mathbf{Z}\,\} = \{\,\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}((2u-v)+\mathrm{i}(u+2v)) \,:\, u,\, v \in \mathbf{Z}\,\} = \{\,4u-2v \,:\, u,\, v \in \mathbf{Z}\,\} = (2)$, wohingegen $(\,\mathrm{Tr}_{\mathbf{Q}(\mathrm{i})|\mathbf{Q}}(2+\mathrm{i})\,) = (4)$ ist.

Ad (6). Die Aussage ist richtig.

Es ist $\mathrm{Tr}_{L|K}(\mathfrak{h}) \subseteq \mathrm{Tr}_{L|K}(\mathfrak{h}_\mathfrak{p})$. Letzteres ist ein gebrochenes Ideal von $A_\mathfrak{p}$; cf. (4). Also ist $\mathrm{Tr}_{L|K}(\mathfrak{h})_\mathfrak{p} \subseteq \mathrm{Tr}_{L|K}(\mathfrak{h}_\mathfrak{p})$.

Ist umgekehrt $x \in \mathrm{Tr}_{L|K}(\mathfrak{h}_\mathfrak{p})$, so können wir $x = \mathrm{Tr}_{L|K}(\frac{h}{s})$ schreiben mit $h \in \mathfrak{h}$ und $s \in A \setminus \mathfrak{p}$. Es wird $x = \mathrm{Tr}_{L|K}(\frac{h}{s}) = s^{-1}\,\mathrm{Tr}_{L|K}(h) \in \mathrm{Tr}_{L|K}(\mathfrak{h})_\mathfrak{p}$, da $s^{-1} \in K$ liegt und da $\mathrm{Tr}_{L|K}$ eine K-lineare Abbildung ist.

Insgesamt ist also $\mathrm{Tr}_{L|K}(\mathfrak{h})_\mathfrak{p} = \mathrm{Tr}_{L|K}(\mathfrak{h})_\mathfrak{p}$.

Ad (7). Die Aussage ist richtig.

Zu zeigen ist nur $A \stackrel{!}{\subseteq} \mathrm{Tr}_{L|K}(B^{\#,A})$; cf. Bemerkung 94.(3).

Es genügt, $1 \overset{!}{\in} \mathrm{Tr}_{L|K}(B^{\#,A})$ zu zeigen; cf. Bemerkung 94.(1) und (4).

Es genügt, $1 \overset{!}{\in} \mathrm{Tr}_{L|K}(B^{\#,A})_{\mathfrak{p}} \overset{(6)}{=} \mathrm{Tr}_{L|K}((B^{\#,A})_{\mathfrak{p}}) \overset{\text{A. 35.(2)}}{=} \mathrm{Tr}_{L|K}((B_{\mathfrak{p}})^{\#,A_{\mathfrak{p}}})$ zu zeigen; cf. (4), Bemerkung 81.(5).

Es ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring, insbesondere also ein Hauptidealbereich; cf. Bemerkung 74. Es ist $B_{\mathfrak{p}} = \Gamma_L(A_{\mathfrak{p}})$; cf. Bemerkung 82.(2).

Also ist o.E. A ein Hauptidealbereich und wir haben $1 \overset{!}{\in} \mathrm{Tr}_{L|K}(B^{\#,A})$ zu zeigen.

Sei $(g_1, \ldots, g_\ell)$ eine A-lineare Basis von B; cf. Lemma 33. Sei $(g'_1, \ldots, g'_\ell)$ die zugehörige duale Basis bezüglich Spurbilinearform; cf. Lemma 22. Es ist $B^{\#,A} = {}_A\langle g'_1, \ldots, g'_\ell \rangle$; cf. Lemma 31.(3).

Es ist $g'_1 \in B^{\#,A}$. Also ist auch $g_1 g'_1 \in B^{\#,A}$; cf. Bemerkung 94.(1). Somit wird

$$\mathrm{Tr}_{L|K}(B^{\#,A}) \ \ni \ \mathrm{Tr}_{L|K}(g_1 g'_1) \ = \ 1 \, .$$

Aufgabe 38

Ad (1). Es ist $\mathfrak{D}_{L|K,A,\mathfrak{p}} \overset{\text{D. 95.(1)}}{=} ((B^{\#,A})^{-1})_{\mathfrak{p}}$.

Es ist $\mathfrak{D}_{L|K,A_{\mathfrak{p}}} \overset{\text{D. 95.(1), L. 70.(4)}}{=} (B_{\mathfrak{p}}^{\#,A_{\mathfrak{p}}})^{-1} \overset{\text{A. 35.(2)}}{=} ((B^{\#,A})_{\mathfrak{p}})^{-1} = ((B^{\#,A})^{-1})_{\mathfrak{p}}$.

Ad (2). Es ist $\mathfrak{d}_{L|K,A,\mathfrak{p}} \overset{\text{D. 95.(2)}}{=} \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A})_{\mathfrak{p}} \overset{\text{L. 87}}{=} \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A,\mathfrak{p}}) \overset{(1)}{=} \mathrm{N}_{L|K}(\mathfrak{D}_{L|K,A_{\mathfrak{p}}}) \overset{\text{D. 95.(2)}}{=} \mathfrak{d}_{L|K,A_{\mathfrak{p}}}$.

Aufgabe 39

Schreibe $B' := \Gamma_{L'}(A)$, $B'' := \Gamma_{L''}(A)$ und $B := \Gamma_L(A)$.

Es genügt, $\mathfrak{d}_{L|K,A,\mathfrak{p}} \overset{!}{=} (\mathfrak{d}^{\ell''}_{L'|K,\,A} \cdot \mathfrak{d}^{\ell'}_{L''|K,A})_{\mathfrak{p}}$ für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$ zu zeigen; cf. Lemma 77.

Dank Aufgaben 38.(2) und 29.(8) bedeutet dies $\mathfrak{d}_{L|K,A_{\mathfrak{p}}} \overset{!}{=} \mathfrak{d}^{\ell''}_{L'|K,\,A_{\mathfrak{p}}} \cdot \mathfrak{d}^{\ell'}_{L''|K,A_{\mathfrak{p}}}$. Nun sind $A_{\mathfrak{p}}$, $B'_{\mathfrak{p}}$, $B''_{\mathfrak{p}}$ und $B_{\mathfrak{p}}$ Hauptidealbereiche; es ist $K = \mathrm{Quot}(A_{\mathfrak{p}})$ sowie $L' = \mathrm{Quot}(B'_{\mathfrak{p}})$, $L'' = \mathrm{Quot}(B''_{\mathfrak{p}})$ und $L = \mathrm{Quot}(B_{\mathfrak{p}})$; es ist $B'_{\mathfrak{p}} = \Gamma_L(A'_{\mathfrak{p}})$, $B''_{\mathfrak{p}} = \Gamma_L(A''_{\mathfrak{p}})$ und $B_{\mathfrak{p}} = \Gamma_L(A_{\mathfrak{p}})$; es ist $\mathfrak{d}_{L'|K,A_{\mathfrak{p}}} + \mathfrak{d}_{L''|K,A_{\mathfrak{p}}} = \mathfrak{d}_{L'|K,A,\mathfrak{p}} + \mathfrak{d}_{L''|K,A,\mathfrak{p}} = (\mathfrak{d}_{L'|K,A} + \mathfrak{d}_{L''|K,A})_{\mathfrak{p}} = (1)$ in $A_{\mathfrak{p}}$ gemäß Aufgaben 38.(2) und 29.(8).

Somit dürfen wir o.E. A, B', B'' und B als Hauptidealbereiche voraussetzen. Wähle eine A-lineare Basis $\underline{g'} = (\, g'_i \,:\, i \in [1, \ell'] \,)$ von B' und eine A-lineare Basis $\underline{g''} = (\, g''_j \,:\, j \in [1, \ell''] \,)$ von B''; cf. Lemma 33. Dann ist $\underline{g} := (\, g'_i g''_j \,:\, i \in [1, \ell'],\, j \in [1, \ell''] \,)$ eine A-lineare Basis von B; cf. Satz 48.(1). Es wird

$$\mathfrak{d}_{L|K,A} \overset{\text{L. 96}}{=} (\Delta_{L|K,\,\underline{g}}) \overset{\text{S. 48.(2)}}{=} (\Delta_{L'|K,\,\underline{g'}})^{\ell''} \cdot (\Delta_{L''|K,\,\underline{g''}})^{\ell'} \overset{\text{L. 96}}{=} \mathfrak{d}^{\ell''}_{L'|K,\,A} \cdot \mathfrak{d}^{\ell'}_{L''|K,A} \, .$$

Aufgabe 40

Vorbemerkung. Es ist $B = \mathbf{Z}[\alpha]$ mit $\alpha := \frac{1}{2}(1 + \sqrt{13})$. Es ist $B' := Z[\alpha']$ mit $\alpha' := \sqrt{3}$. Cf. Aufgabe 3.

Mit der Lösung zu Aufgabe 16.(2) folgt $\Delta_L = 13$, $\Delta_{L'} = 2^2 \cdot 3$ und $\Delta_M = 2^4 \cdot 3^2 \cdot 13^2$.

Diese Diskriminanten sind teilerfremd und es sind $L|K$ und $L'|K$ linear disjunkt; cf. Lösung zu Aufgabe 16.(2). Dank Satz 48 ist also $C = \mathbf{Z}[\alpha, \alpha']$.

Ad (1). Es ist $\mu_{\alpha,K}(X) = X^2 - X - 3$. Also ist $\mu'_{\alpha,K}(X) = 2X - 1$. Folglich ist $\mu'_{\alpha,K}(\alpha) = 2\alpha - 1$. Dank Lemma 97 ist also $\mathfrak{D}_{L|K,A} = (2\alpha - 1) = (\sqrt{13}) \in \mathrm{Ideale}^{\times}(B)$.

Es ist $\mu_{\alpha',K}(X) = X^2 - 3$. Da $L|K$ und $L'|K$ linear disjunkt sind, ist auch $\mu_{\alpha',L}(X) = X^2 - 3$; cf.

Definition 43. Also ist $\mu'_{\alpha',L}(X) = 2X$. Folglich ist $\mu'_{\alpha',L}(\alpha') = 2\alpha'$. Dank Lemma 97 ist also $\mathfrak{D}_{M|L,B} = (2\alpha') \in \text{Ideale}^\times(C)$.

Dank Satz 100 folgt $\mathfrak{D}_{M|K,A} = ((2\alpha-1)\cdot 2\alpha') = (2\sqrt{13}\cdot\sqrt{3}) \in \text{Ideale}^\times(C)$.

Ad (2). Es ist $\mu_{\alpha,K}(X) = X^2 - X - 3$. Da $L|K$ und $L'|K$ linear disjunkt sind, ist auch $\mu_{\alpha,L'}(X) = X^2 - X - 3$; cf. Definition 43. Also ist $\mu'_{\alpha,L'}(X) = 2X - 1$. Folglich ist $\mu'_{\alpha,L'}(\alpha) = 2\alpha - 1$. Dank Lemma 97 ist also $\mathfrak{D}_{M|L',A} = (2\alpha - 1) = (\sqrt{13}) \in \text{Ideale}^\times(C)$.

Es ist $\mu_{\alpha',K}(X) = X^2 - 3$. Also ist $\mu'_{\alpha',K}(X) = 2X$. Folglich ist $\mu'_{\alpha',K}(\alpha') = 2\alpha'$. Dank Lemma 97 ist also $\mathfrak{D}_{L'|K,B} = (2\alpha') = (2\sqrt{13}) \in \text{Ideale}^\times(B')$.

Dank Satz 100 folgt $\mathfrak{D}_{M|K,A} = ((2\alpha-1)\cdot 2\alpha') \in \text{Ideale}^\times(C)$.

Ad (3). Es ist $\mathfrak{d}_{L|K,A} = \mathrm{N}_{L|K}(\,(2\alpha-1)\,) = \mathrm{N}_{L|K}(\,(\sqrt{13})\,) = (\sqrt{13}\cdot(-\sqrt{13})) = (-13) = (13)$, in Übereinstimmung mit $\Delta_L = 13$ von oben.

Es ist $\mathfrak{d}_{L'|K,A} = \mathrm{N}_{L'|K}(\,(2\alpha')\,) = (2\alpha'\cdot 2(-\alpha')) = (-4\cdot 3) = (2^2\cdot 3)$, in Übereinstimmung mit $\Delta_L = 2^2\cdot 3$ von oben.

Es ist $\mathfrak{d}_{M|K,A} = \mathrm{N}_{M|K}(\,((2\alpha-1)\cdot 2\alpha')\,) = \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\,((2\alpha-1)\cdot 2\alpha')\,) = \mathrm{N}_{L|K}(\,((2\alpha-1)^2\cdot 2\alpha'\cdot 2(-\alpha'))\,) = \mathrm{N}_{L|K}(\,((2\alpha-1)^2\cdot 2^2\cdot 3\,) = (((2\alpha-1)^2(2(1-\alpha)-1)^2\cdot(2^2\cdot 3)^2) = (13^2\cdot 2^4\cdot 3^2)$, in Übereinstimmung mit $\Delta_L = 2^4\cdot 3^2\cdot 13^2$ von oben.

Aufgabe 41

Für $w \in V$ und $r \in \mathbf{R}_{>0}$ schreiben wir noch $\overline{\mathrm{B}}_r(w) := \{\, v \in V \,:\, \|v-w\| \leqslant r \,\}$.

Ad (1) $\Rightarrow$ (2). In $\mathrm{B}_1(x)$ gibt es nur endlich viele Elemente aus X. Also gibt es ein $\varepsilon \in \mathbf{R}_{>0}$ mit $\varepsilon \leqslant 1$ und $\varepsilon < \|y-x\|$ für alle $y \in \overline{\mathrm{B}_1(v)} \smallsetminus \{v\}$. Daher ist dann auch $\mathrm{B}_\varepsilon(v) \cap X = \{v\}$.

Ad (2) $\Rightarrow$ (1). Seien $r \in \mathbf{R}_{>0}$ und $w \in V$ gegeben. Es genügt zu zeigen, daß $X \cap \overline{\mathrm{B}}_r(w)$ endlich ist. *Annahme,* dem ist nicht so. Wir bilden eine Folge $(x_i)_{i\geqslant 1}$ mit $x_i \in X \cap \overline{\mathrm{B}}_r(w)$ und $x_i \neq x_j$ für $i \neq j$ stets. Es ist $\overline{\mathrm{B}}_r(w)$ folgenkompakt; cf. [**9,** §4.2.5, §4.2.6]. Also konvergiert diese Folge gegen ein $v \in \overline{\mathrm{B}}_r(w)$. Dann ist für alle $\varepsilon \in \mathbf{R}_{>0}$ die Menge $(\mathrm{B}_\varepsilon(v) \smallsetminus \{v\}) \cap X$ nichtleer, da in ihr unendlich viele Folgenglieder liegen. Wir haben einen *Widerspruch.*

Sei nun X eine Untergruppe.

Ad (2) $\Rightarrow$ (3). Wende (2) mit $v = 0$ an.

Ad (3) $\Rightarrow$ (2). O.E. ist $\{0\} \subset X$.

Annahme, für alle $\varepsilon \in \mathbf{R}_{>0}$ ist $(\mathrm{B}_\varepsilon(v) \smallsetminus \{v\}) \cap X \neq \emptyset$. Wähle $x_1 \in X \smallsetminus \{v\}$. Für $i \geqslant 1$ wähle rekursiv ein $x_i \in (\mathrm{B}_{\min\{\|x_{i-1}-v\|,1/i\}}(v) \smallsetminus \{v\}) \cap X$. Dann ist $(x_i)_{i\geqslant 1}$ eine Folge mit $x_i \in X$, $x_i \neq x_j$ für $i \neq j$ und $\|x_i - v\| < 1/i$ stets. Sei $x'_i := x_i - x_{i+1}$ für $i \geqslant 1$. Es ist $x'_i \in X \smallsetminus \{0\}$ und

$$\|x'_i\| \;=\; \|x_i - x_{i+1}\| \;\leqslant\; \|x_i - v\| + \|v - x_{i+1}\| \;<\; 2/i$$

stets. Also ist für alle $\varepsilon \in \mathbf{R}_{>0}$ die Menge $(\mathrm{B}_\varepsilon(0) \smallsetminus \{0\}) \cap X$ nichtleer. Wir haben einen *Widerspruch.*

Ad (1) $\Rightarrow$ (4). Dies folgt durch Anwendung von Definition 105 mit $w = 0$.

Ad (4) $\Rightarrow$ (3). Sei $\varepsilon := \min\{\, \|x\| \,:\, x \in (\mathrm{B}_r(0) \smallsetminus \{0\}) \cap X \,\}$. Dann ist $\mathrm{B}_\varepsilon(0) \cap X = \{0\}$.

Aufgabe 42

Sei $z \in \mathbf{K}_\mathbf{R}$ gegeben. Schreiben wir $z \in K_\mathbf{R}$ als $\mathbf{R}$-Linearkombination in der Orthonormalbasis aus

Bemerkung 112.(1, 2), i.e. als

$$z \;=\; \big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{R}}(K)} a_\tau(\partial_{\tau,\sigma})_\sigma\big) + \big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} u_\tau(2^{-1/2}(\partial_{\tau,\sigma}+\partial_{\bar\tau,\sigma}))_\sigma\big) + \big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} v_\tau(2^{-1/2}(\mathrm{i}\partial_{\tau,\sigma}-\mathrm{i}\partial_{\bar\tau,\sigma}))_\sigma\big)$$

mit $a_\tau\,,\ u_\tau\,,\ v_\tau\ \in \mathbf{R}$ stets, dann wird

$$\mathrm{Tr}(z) \;=\; \big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{R}}(K)} a_\tau\big) + 2^{1/2}\big(\sum_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} u_\tau\big)$$

und

$$\mathrm{N}(z) \;=\; \big(\prod_{\tau\in\mathrm{Einb}_{\mathbf{R}}(K)} a_\tau\big)\cdot 2^{-s}\big(\prod_{\tau\in\mathrm{Einb}_{\mathbf{C}}(K)} (u_\tau^2+v_\tau^2)\big)\,.$$

Beides sind Polynome in den Koordinaten bezüglich unserer Orthonormalbasis. Also sind Tr und N stetig.

> Ausführlicher. Sei $\mathbf{R}^k$, gesehen als euklidischer Raum mit dem Standardskalarprodukt. Die Abbildung $\varphi : K_{\mathbf{R}} \to \mathbf{R}^k$, die jedem Element aus $K_{\mathbf{R}}$ seinen Koordinatenvektor bezüglich unserer Orthonormalbasis zuordnet, ist ein Isomorphismus von euklidischen Räumen, insbesondere also eine bijektive stetige Abbildung mit stetiger Umkehrabbildung $\varphi^{-1} : \mathbf{R}^k \to K_{\mathbf{R}}$. Wir haben gezeigt, daß $\mathrm{Tr}\circ\varphi^{-1}$ und $\mathrm{N}\circ\varphi^{-1}$ als Polynome auf dem euklidischen Standardraum $\mathbf{R}^k$ stetige Abbildungen sind. Also sind auch $\mathrm{Tr} = \mathrm{Tr}\circ\varphi^{-1}\circ\varphi$ und $\mathrm{N} = \mathrm{N}\circ\varphi^{-1}\circ\varphi$ stetig.

Aufgabe 43

Ad (1). Es ist $\mathfrak{p} \subseteq A\cap\mathfrak{q}$. Da $\mathfrak{p}\subset A$ ein maximales Ideal ist und da $1\notin\mathfrak{q}$, also auch $1\notin A\cap\mathfrak{q}$ liegt, folgt $\mathfrak{p} = A\cap\mathfrak{q}$; cf. Definition 52.

Es sind $B/\mathfrak{q}$ und $A/\mathfrak{p}$ Körper. Ferner haben wir den Körpermorphismus $A/\mathfrak{p}\to B/\mathfrak{q}$, $a+\mathfrak{p}\mapsto a+\mathfrak{q}$, den wir als Einbettung ansehen wollen.

Dank Aufgabe 32.(1) ist B ein endlich erzeugter A-Modul. Schreibe demgemäß $B = {}_A\langle b_1\,,\,\ldots\,,\,b_m\rangle$ mit $m\geqslant 0$ und $b_i\in B$ für $i\in[1,m]$. Dann ist $B/\mathfrak{q} = {}_{A/\mathfrak{p}}\langle b_1+\mathfrak{q}\,,\,\ldots\,,\,b_m+\mathfrak{q}\rangle$, da sich jedes Element $b+\mathfrak{q}\in B/\mathfrak{q}$ schreiben läßt als

$$\begin{aligned} b+\mathfrak{q} &= (\textstyle\sum_{i\in[1,m]} a_ib_i)+\mathfrak{q}\\ &= \textstyle\sum_{i\in[1,m]}(a_i+\mathfrak{q})(b_i+\mathfrak{q})\\ &= \textstyle\sum_{i\in[1,m]}(a_i+\mathfrak{p})\cdot(b_i+\mathfrak{q})\end{aligned}$$

mit $a_i\in A$ für $i\in[1,m]$.

Zeigen wir nun $\mathrm{N}_{L|K}(\mathfrak{q}) \stackrel{!}{=} \mathfrak{p}^f$. Es genügt, $\mathrm{N}_{L|K}(\mathfrak{q})_{\mathfrak{t}} \stackrel{!}{=} (\mathfrak{p}^f)_{\mathfrak{t}}$ für $\mathfrak{t}\in\mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$ zu zeigen; cf. Lemma 77.

Dank Lemma 88 und Aufgabe 29.(8) genügt es, $\mathrm{N}_{L|K}(\mathfrak{q}_{\mathfrak{t}}) \stackrel{!}{=} (\mathfrak{p}_{\mathfrak{t}})^f$ zu zeigen.

Fall $\mathfrak{t}\neq\mathfrak{p}$. Es ist $\mathfrak{p}\not\subseteq\mathfrak{t}$, da es sich um zwei verschiedene maximale Ideale handelt; cf. Definition 52. Sei $s\in\mathfrak{p}\smallsetminus\mathfrak{t}$. Dann ist s eine Einheit von $A_{\mathfrak{t}}$, die in $\mathfrak{p}_{\mathfrak{t}}$ liegt. Folglich ist $\mathfrak{p}_{\mathfrak{t}} = (1)$. Ferner ist s eine Einheit in $B_{\mathfrak{t}}$, die in $\mathfrak{q}_{\mathfrak{t}}$ liegt; cf. Bemerkung 82. Also ist auch $\mathrm{N}_{L|K}(\mathfrak{q}_{\mathfrak{t}}) = \mathrm{N}_{L|K}(\,(1)\,) = (\,\mathrm{N}_{L|K}(1)\,) = (1)$; cf. Bemerkung 86.(3).

Fall $\mathfrak{t}=\mathfrak{p}$. Nun sind $A_{\mathfrak{p}}$ und $B_{\mathfrak{p}}$ Hauptidealbereiche und es ist $K = \mathrm{Quot}(A_{\mathfrak{p}})$ sowie $L = \mathrm{Quot}(B_{\mathfrak{p}})$, und es ist $B_{\mathfrak{p}} = \Gamma_L(A_{\mathfrak{p}})$; cf. Bemerkung 82.(1, 2, 3). Desweiteren ist $A/\mathfrak{p}\stackrel{\sim}{\to} A_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$, $a+\mathfrak{p}\mapsto a+\mathfrak{p}_{\mathfrak{p}}$; cf. Aufgabe 10.(2).

Ferner ist $B/\mathfrak{q}\stackrel{\sim}{\to} B_{\mathfrak{p}}/\mathfrak{q}_{\mathfrak{p}}$, $b+\mathfrak{q}\mapsto b+\mathfrak{q}_{\mathfrak{p}}$. Es ist ein Ringmorphismus. Zeigen wir die Injektivität. Sei $b\in\mathfrak{q}_{\mathfrak{p}}$, i.e. sei $b=\frac{q}{s}$ für ein $q\in\mathfrak{q}$ und ein $s\in A\smallsetminus\mathfrak{p}$. Dann wird $bs = q\in\mathfrak{q}$. Es ist $s\in A\smallsetminus\mathfrak{p} = A\smallsetminus(A\cap\mathfrak{q})\subseteq B\smallsetminus\mathfrak{q}$.

Wegen $\mathfrak{q}$ prim ist also $b \in \mathfrak{q}$. (Wegen $B/\mathfrak{q}$ Körper hätte die Injektivität auch nur im Falle $\mathfrak{q}_\mathfrak{p} = B_\mathfrak{p}$ verletzt sein können.) Zeigen wir die Surjektivität. Sei $\frac{b}{s} + \mathfrak{q}_\mathfrak{p}$ gegeben, wobei $b \in B$ und $s \in A \setminus \mathfrak{p}$ sei. Wir suchen ein $b' \in B$ mit $\frac{b}{s} + \mathfrak{q} = b' + \mathfrak{q}$, i.e. mit $b = sb' + q$ für ein $q \in \mathfrak{q}$. Es ist $s \in A \setminus \mathfrak{p} = A \setminus (A \cap \mathfrak{q}) \subseteq B \setminus \mathfrak{q}$. Wegen $\mathfrak{q} \subset B$ maximal folgt aber $(s) + \mathfrak{q} = B$.

Somit dürfen wir o.E. A und B als Hauptidealbereiche voraussetzen. Es ist B ein freier A-Modul von Rang ℓ; cf. Lemma 33. Schreibe $\mathfrak{p} = (p)$ mit $p \in A$ und $\mathfrak{q} = (q)$ mit $q \in B$. Betrachten wir die A-lineare Abbildung $\lambda_q : B \to B$, $y \mapsto qy$. Nach Elementarteilersatz gibt es eine A-lineare Basen von B so, daß dererbezüglich diese Abbildung durch eine Matrix der Form $D = \mathrm{diag}(d_1 , \ldots , d_\ell)$ gegeben ist mit $d_i \in A$ für $i \in [1, \ell]$.

Es ist $B/(q) = B/\lambda_b(B) \simeq \bigoplus_{i\in[1,\ell]} A/(d_i)$. Wegen $p \in (q)$ ist $p(B/(q)) = 0$ und also $p(A/(d_i)) = 0$, i.e. $(p) \subseteq (d_i)$ für $i \in [1, \ell]$. Also ist $(d_i) = (p)$ oder $(d_i) = (1)$ stets. Es folgt $f = \dim_{A/(p)} B/(q) = |\{\, i \in [1, \ell] : (d_i) = (p) \,\}|$ und somit

$$\mathrm{N}_{L|K}(\,(q)\,) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{L|K}(q)\,) \;=\; (\,\det(D)\,) \;=\; \prod_{i\in[1,\ell]} (\,d_i\,) \;=\; (p^f)\,.$$

Cf. auch Beweis zu Lemma 54.

Ad (2). Zum einen ist $\mathrm{N}_{L|K}(\mathfrak{p}B) = \mathfrak{p}^\ell$; cf. Aufgabe 34.(3). Zum anderen ist

$$\begin{array}{rcl}
\mathfrak{p}^\ell & \overset{\text{A. 34.(3)}}{=} & \mathrm{N}_{L|K}(\mathfrak{p}B) \\
& = & \mathrm{N}_{L|K}(\textstyle\prod_{i\in[1,d]} \mathfrak{q}_i^{e_i}) \\
& \overset{\text{L. 88}}{=} & \textstyle\prod_{i\in[1,d]} \mathrm{N}_{L|K}(\mathfrak{q}_i)^{e_i} \\
& \overset{(1)}{=} & \textstyle\prod_{i\in[1,d]} (\mathfrak{p}^{f_i})^{e_i} \\
& = & \mathfrak{p}^{\sum_{i\in[1,d]} e_i f_i}
\end{array}$$

und folglich

$$\ell \;=\; \sum_{i\in[1,d]} e_i f_i\,;$$

cf. Satz 63.(2).

Aufgabe 44

Ad (1). Schreibe $\mu(X) = X^m + \sum_{i\in[0,m-1]} a_i X^i$ mit $a_i \in R$ stets. Schreibe $\bar\mu(X) \in (R/(r))[X]$ für sein Bild unter der koeffizientenweise angewandten Restklassenabbildung.

Ad $\Rightarrow$. Sei S ein diskreter Bewertungsring mit maximalem Ideal erzeugt von s. In S schreiben wir $(r) = (s^e)$ für ein $e \in \mathbf{Z}_{\geqslant 1}$. Gemäß Aufgabe 43.(2) ist $m = ef$, wobei $f := \dim_{R/(r)}(S/(s))$ ist.

Insbesondere ist $s^m \equiv_r 0$. Somit erhalten wir einen wohldefinierten Ringmorphismus

$$\bar\varphi \;:\; (R/(r))[X]/(X^m) \xrightarrow{\;\bar\varphi\;} S/(r)$$

mit $\bar\varphi(x + (r)) = x + (r)$ für $x \in R$ und mit $\bar\varphi(X) = s + (r)$. Es ist $\bar\varphi$ surjektiv, da $S = R[s]$. Es ist $\bar\varphi$ eine $R/(r)$-lineare Abbildung. Es ist $\dim_{R/(r)}(R/(r))[X]/(X^m) = m$. Da $(s^i : i \in [0, m-1])$ eine R-lineare Basis von S ist, ist $(s^i + (r) : i \in [0, m-1])$ eine $R/(r)$-lineare Basis von $S/(r)$. Insbesondere ist $\dim_{R/(r)} S/(r) = m$. Folglich ist $\bar\varphi$ ein Ringisomorphismus.

Somit ist $s^k + (r) \neq 0 + (r)$ für $k \in [0, m-1]$. Damit muß $e = m$ sein und $f = 1$. Letzteres hat den Körperisomorphismus $R/(r) \xrightarrow{\sim} S/(s)$, $x + (r) \mapsto x + (s)$ zur Folge.

Da $\bar{\mu}(X)+(X^m)$ unter $\bar{\varphi}$ auf $\mu(s)+(r)=0$ kommt, ist bereits $\bar{\mu}(X)+X^m=0$, i.e. es ist X^m ein Teiler von $\bar{\mu}(X)$. Da $\bar{\mu}(X)$ ein normiertes Polynom von Grad m ist, folgt $\bar{\mu}(X)=X^m$, i.e. $\mu(X)\equiv_r X^m$. Ferner ist $\mathrm{v}_s(x)=m\,\mathrm{v}_r(x)$ für $x\in R$.

Es bleibt zu zeigen, daß $a_0=\mu(0)\overset{!}{\not\equiv}_{r^2}0$ ist. Es ist $s^m=-\sum_{i\in[0,m-1]}a_is^i$, also $m=\mathrm{v}_s(s^m)=\mathrm{v}(-\sum_{i\in[0,m-1]}a_is^i)$. Da die Bewertungen der Koeffizienten bei s Vielfache von m sind, sind die Bewertungen bei s der auftretenden Summanden paarweise verschieden. Es folgt $m=\min\{\,\mathrm{v}_s(a_i)+i\,:\,i\in[0,m-1]\,\}$; cf. Aufgabe 2.(5). Dies ist nur möglich, wenn dieses Minimum bei $i=0$ angenommen wird. Dies zieht $m=\mathrm{v}_s(a_0)$ und also $1=\mathrm{v}_r(a_0)$ nach sich, i.e. $a_0\equiv_r 0$, aber $a_0\not\equiv_{r^2}0$.

Dieses Minimumsargument zeigt abermals, daß $\mathrm{v}_s(a_i)\geqslant m$, i.e. $\mathrm{v}_r(a_i)\geqslant 1$ ist für $i\in[0,m-1]$.

Ad $\Leftarrow$. Sei nun umgekehrt $\mu(X)$ eisensteinsch. Wir behaupten, daß S ein diskreter Bewertungsring mit maximalem Ideal erzeugt von s ist.

Es ist S kein Körper, da ansonsten $s^{-1}=\sum_{i\in[0,m-1]}b_is^i$ für gewisse $b_i\in R$ wäre, was nach sich zöge, daß $-1+\sum_{i\in[0,m-1]}b_is^{i+1}=0$ und also $\mu(X)$ ein Teiler von $1-\sum_{i\in[0,m-1]}b_iX^{i+1}$ wäre. Aus Gradgründen wäre $1-\sum_{i\in[0,m-1]}b_iX^{i+1}=b_m\mu(X)$ und insbesondere $1=b_ma_0$. Dies aber ist wegen $a_0\in(r)$ nicht möglich.

Sei $\mathfrak{m}\subseteq S$ ein maximales Ideal. Da S kein Körper ist, ist $\mathfrak{m}\neq(0)$. Wähle $y\in\mathfrak{m}$. Da $y\in S\subseteq\Gamma_L(R)$, ist $\mu_{y,K}(X)\in R[X]$. Der konstante Term von $\mu_{y,K}(X)$ liegt wegen $\mu_{y,K}(y)=0$ in $(y)\subseteq\mathfrak{m}\subset S$ und somit auch in $\mathfrak{m}\cap R$. Da dieser konstante Term nicht gleich 0 ist, folgt $\mathfrak{m}\cap R\neq(0)$. Da $\mathfrak{m}\cap R$ ein Primideal von R ist und da $\mathrm{Ideale}^{\times}_{\mathrm{prim}}(R)=\{(r)\}$ ist, folgt $\mathfrak{m}\cap R=(r)$.

Wir haben einen Ringisomorphismus $(R/(r))[X]/(X^m)=(R/(r))[X]/(\bar{\mu}(X))\xrightarrow{\sim}S/(r)$, $X+(\mu(X))\mapsto s+(r)$; cf. Aufgabe 30.(2.i). Die maximalen Ideale von S sind die Urbilder der maximalen Ideale von $S/(r)$. Es hat $(R/(r))[X]/(X^m)$ nur das maximale Ideal $(X+(X^m))$, da im Hauptidealbereich $(R/(r))[X]$ ein maximales Ideal, das X^m enthält, von einem irreduziblen Teiler von X^m erzeugt werden muß und also gleich (X) ist. Somit hat $S/(r)$ nur das maximale Ideal $(s+(r))$. Also hat S nur das maximale Ideal $(s,r)\subset S$.

Wegen $\mu(s)=0$ ist $a_0\in(s)$, wegen $(r)=(a_0)$ also auch $r\in(s)$ und somit $(s)=(s,r)$.

Insgesamt ist (s) das einzige maximale Ideal in S.

Es ist $S\smallsetminus(s)=\mathrm{U}(S)$, da für $x\in S\smallsetminus(s)$ das Ideal (x) in keinem maximalen Ideal enthalten ist, also gleich S sein muß; cf. Bemerkung 51.(4), beachte R noethersch, also $R[X]$ noethersch nach Aufgabe 24.(2), also $R[s]$ noethersch nach Aufgabe 24.(3).

Wir *behaupten* $s^mr^{-1}\overset{!}{\in}\mathrm{U}(S)$. Wegen $s^m=-\sum_{i\in[0,m-1]}a_is^i$ ist $s^m\in(r)\subset S$, i.e. $s^mr^{-1}\in S$. Da $\sum_{i\in[1,m-1]}(a_ir^{-1})s^i\in(s)$ und $a_0r^{-1}\in\mathrm{U}(R)\subseteq\mathrm{U}(S)=S\smallsetminus(s)$, ist $s^mr^{-1}=a_0r^{-1}+\sum_{i\in[1,m-1]}(a_ir^{-1})s^i\in S\smallsetminus(s)=\mathrm{U}(S)$. Dies zeigt die *Behauptung*.

Sei $x=\sum_{i\in[0,m-1]}b_is^i\in S^\times$ gegeben, wobei $b_i\in R$ für $i\in[0,m-1]$. Sei $v:=\min\{\,\mathrm{v}_r(b_i)\,:\,i\in[0,m-1]\,\}$. Sei $j:=\min\{\,i\in[0,m-1]\,:\,\mathrm{v}_r(b_i)=v\,\}$. Es ist $b_j\neq0$. Es ist $r^{-v}b_j\in\mathrm{U}(R)\subseteq\mathrm{U}(S)$, insbesondere $r^{-v}b_j\notin(s)$. Für $i\in[0,j-1]$ ist $r^{-v}b_is^{i-j}=(r^{-v-1}b_i)(rs^{-m})s^{i-j+m}\in(s)$. Für $i\in[j+1,m-1]$ ist $r^{-v}b_is^{i-j}=(r^{-v}b_is^{i-j-1})s\in(s)$. Also ist

$$s^{-j}r^{-v}x\;=\;(\textstyle\sum_{i\in[0,j-1]}r^{-v}b_is^{i-j})+r^{-v}b_j+(\sum_{i\in[j+1,m-1]}r^{-v}b_is^{i-j})\;\in\;S\smallsetminus(s)\;=\;\mathrm{U}(S)\,.$$

Da $r^{-v}s^{vm}\in\mathrm{U}(S)$, ist damit auch

$$s^{-j-vm}x\;\in\;\mathrm{U}(S)\,.$$

Somit ist

$$(x)\;=\;(s^{j+vm})\,.$$

Für $k \geqslant 2$ ist (s^k) nicht prim, da $s \cdot s^{k-1} \in (s^k)$, aber $s \notin (s^k)$ und $s^{k-1} \notin (s^k)$.

Folglich ist S ein Hauptidealbereich mit $\text{Ideale}^{\times}_{\text{prim}} = \{(s)\}$, i.e. ein diskreter Bewertungsring mit maximalem Ideal erzeugt von s.

Ad (2). Im Falle $R = \mathbf{Z}_{(p)}$, $r = p$, $s = \zeta_p - 1$ ist sowohl $R[s] = \mathbf{Z}_{(p)}[\zeta_p]$ ein diskreter Bewertungsring mit maximalem Ideal erzeugt von $s = \zeta_p - 1$, da

$$\mu_{\zeta_p - 1, \mathbf{Q}}(X) \;=\; \Phi_p(X+1) \;=\; \frac{(X+1)^p - 1}{(X+1) - 1} \;=\; \sum_{j \in [0, p-1]} \tbinom{p}{j+1} X^j$$

eisensteinsch ist.

Cf. auch das spätere Lemma 129.(3) im Falle $\alpha = 1$.

Ad (3). Beachte zunächst, daß $\mu_{\zeta_{p^2}, \mathbf{Q}(\zeta_p)}(X) = X^p - \zeta_p$ ist, da dies ein normiertes Polynom in $\mathbf{Q}(\zeta_p)[X]$ mit Nullstelle ζ_{p^2} ist und da $[\mathbf{Q}(\zeta_p)(\zeta_{p^2}) : \mathbf{Q}(\zeta_p)] = p$ ist; cf. Aufgabe 17.(1).

Im Falle $R = \mathbf{Z}_{(p)}[\zeta_p]$, $r = \zeta_p - 1$, $s = \zeta_{p^2} - 1$ ist $R[s] = \mathbf{Z}_{(p)}[\zeta_{p^2}]$ ein diskreter Bewertungsring mit maximalem Ideal erzeugt von $s = \zeta_{p^2} - 1$, da

$$\mu_{\zeta_{p^2} - 1, \mathbf{Q}(\zeta_p)}(X) \;=\; \mu_{\zeta_{p^2}, \mathbf{Q}(\zeta_p)}(X+1) \;=\; (X+1)^p - \zeta_p \;=\; \left(\sum_{j \in [1,p]} \tbinom{p}{j} X^j \right) - (\zeta_p - 1)$$

eisensteinsch ist.

Aufgabe 45

Ad (1). Falls $m \geqslant 1$, dann schreibe $v' := (v_i)_{i \in [1, m-1]}$. Es ist

$$\text{vol}(Z_{u,v}) \;=\; \int_0^{2^{1/2} v_i} \text{vol}(Z_{u,v'}) \cdot 2\pi t \mathrm{d}\, t \;=\; \text{vol}(Z_{u,v'}) \cdot \pi 2 v_i^2 \;.$$

Falls $n \geqslant 1$, dann schreibe $u' := (u_i)_{i \in [1, n-1]}$. Es ist

$$\text{vol}(Z_{u,v}) \;=\; \int_{-u_i}^{u_i} \text{vol}(Z_{u',v}) \mathrm{d}\, t \;=\; \text{vol}(Z_{u',v}) \cdot 2u_i \;.$$

Unter Verwendung von $\text{vol}(Z_{(),()}) = 1$ liefert dies aufmultipliziert also

$$\text{vol}(Z_{u,v}) \;=\; 2^{n+m} \Big(\prod_{i \in [1,n]} u_i \Big) \Big(\prod_{i \in [1,m]} v_i^2 \Big) \;.$$

Ad (2). Für $n \geqslant 1$ und $m \geqslant 0$ ist

$$\text{vol}(M_{n,m,R}) \;=\; \int_{-R}^{+R} \text{vol}(M_{n-1,m,R-|t|}) \mathrm{d}\, t \;=\; 2 \int_0^R \text{vol}(M_{n-1,m,t}) \mathrm{d}\, t$$

Für $m \geqslant 1$ ist

$$\text{vol}(M_{0,m,R}) \;=\; \int_0^{2^{-1/2} R} \text{vol}(M_{0,m-1,R-2^{1/2}t}) \cdot 2\pi t \mathrm{d}\, t \;=\; 2\pi \int_0^{2^{-1/2} R} \text{vol}(M_{0,m-1,2^{1/2}t}) \cdot (2^{-1/2} R - t) \mathrm{d}\, t$$

Wir zeigen $\mathrm{vol}(M_{0,m,R}) = \pi^m \frac{R^{2m}}{(2m)!}$ bei festem $R \in \mathbf{R}_{\geqslant 0}$ durch Induktion über $m \geqslant 0$. Für $m = 0$ sind beide Seiten gleich 1. Sei $m \geqslant 1$. Es wird

$$\begin{aligned}
\mathrm{vol}(M_{0,m,R}) &= 2\pi \textstyle\int_0^{2^{-1/2}R} \mathrm{vol}(M_{0,m-1,2^{1/2}t}) \cdot (2^{-1/2}R - t)\mathrm{d}\,t \\
&= 2\pi \textstyle\int_0^{2^{-1/2}R} \pi^m \frac{(2^{1/2}t)^{2m}}{(2m)!}(2^{-1/2}R - t)\mathrm{d}\,t \\
&= 2^{m+1}\pi^{m+1} \tfrac{1}{(2m)!} \textstyle\int_0^{2^{-1/2}R} t^{2m}(2^{-1/2}R - t)\mathrm{d}\,t \\
&= 2^{m+1}\pi^{m+1} \tfrac{1}{(2m)!} \big[\tfrac{1}{2m+1} t^{2m+1} \cdot 2^{-1/2}R - \tfrac{1}{2m+2} t^{2m+2}\big]_{t=0}^{t=2^{-1/2}R} \\
&= 2^{m+1}\pi^{m+1} \tfrac{1}{(2m)!} (\tfrac{1}{2m+1} R^{2m+2} \cdot 2^{-m-1} - \tfrac{1}{2m+2} R^{2m+2} \cdot 2^{-m-1}) \\
&= \pi^{m+1} \tfrac{R^{2(m+1)}}{(2m)!} (\tfrac{1}{2m+1} - \tfrac{1}{2m+2}) \\
&= \pi^{m+1} \tfrac{R^{2(m+1)}}{(2m)!} \tfrac{(2m+2)-(2m+1)}{(2m+1)(2m+2)} \\
&= \pi^{m+1} \tfrac{R^{2(m+1)}}{(2(m+1))!} \ .
\end{aligned}$$

Wir zeigen $\mathrm{vol}(M_{n,m,R}) = 2^n\pi^m \frac{R^{n+2m}}{(n+2m)!}$ bei festem $R \in \mathbf{R}_{\geqslant 0}$ und festen $m \geqslant 0$ durch Induktion über $n \geqslant 0$. Für $n = 0$ ist dies eben gezeigt worden. Sei $n \geqslant 1$. Es wird

$$\begin{aligned}
\mathrm{vol}(M_{0,m,R}) &= 2 \textstyle\int_0^R \mathrm{vol}(M_{n-1,m,t})\mathrm{d}\,t \\
&= 2 \textstyle\int_0^R 2^n\pi^m \frac{t^{n+2m}}{(n+2m)!}\mathrm{d}\,t \\
&= 2^{n+1}\pi^m \textstyle\int_0^R \frac{t^{n+2m}}{(n+2m)!}\mathrm{d}\,t \\
&= 2^{n+1}\pi^m \big[\tfrac{t^{(n+1)+2m}}{((n+1)+2m)!}\big]_0^R \\
&= 2^{n+1}\pi^m \tfrac{R^{(n+1)+2m}}{((n+1)+2m)!} \ .
\end{aligned}$$

Aufgabe 46

Beachte zunächst, daß $\exp(x) \geqslant 1 + x$ ist für $x \in \mathbf{R}$, da für $x = 0$ die beiden Seiten gleich 1 sind und da für $x \geqslant 0$ die Ableitungen $\exp(x) \geqslant 1$, für $x \leqslant 0$ dagegen $\exp(x) \leqslant 1$ erfüllen.

Sei $\bar{a} := \frac{1}{m} \sum_{i\in[1,m]} a_i$. Es ist $\exp(a_i\,\bar{a}^{-1} - 1) \geqslant a_i\,\bar{a}^{-1}$ für $i \in [1, m]$. Es folgt

$$1 \ = \ \exp((\textstyle\sum_{i\in[1,m]} a_i)\bar{a}^{-1} - m) \ = \ \prod_{i\in[1,m]} \exp(a_i\,\bar{a}^{-1} - 1) \ \geqslant \ \prod_{i\in[1,m]} (a_i\,\bar{a}^{-1}) \ = \ (\textstyle\prod_{i\in[1,m]} a_i)\bar{a}^{-m} \ ,$$

und somit $\bar{a}^m \geqslant \prod_{i\in[1,m]} a_i$, i.e. $\bar{a} \geqslant (\prod_{i\in[1,m]} a_i)^{1/m}$.

Dieses Argument stammt von George Polya.

Aufgabe 47

Ad (1). Wir haben, in Standardbezeichnungen, die Minkowskischranke

$$\xi_{\mathbf{Q}(\sqrt{-23})} \ = \ \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\sqrt{-23})}|^{1/2} \ = \ \frac{1}{2} \cdot \frac{4}{\pi} \cdot |-23|^{1/2} \ \approx 3{,}0531 \ ;$$

cf. Definition 115, Aufgabe 16.(1).

Sei $\alpha := \frac{1}{2}(1+\sqrt{-23})$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{-23})} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Wir haben also $\mathrm{Cl}(\mathbf{Z}[\alpha]) \overset{!}{\simeq} \mathrm{C}_3$ zu zeigen. Dank Aufgabe 36.(1) gibt es ein Element der Ordnung 3 in $\mathrm{Cl}(\mathbf{Z}[\alpha])$. Also genügt es, $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \overset{!}{\leqslant} 3$ zu zeigen. Da 3 ein Teiler von $|\mathrm{Cl}(\mathbf{Z}[\alpha])|$ ist, genügt es hierfür, $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \overset{!}{\leqslant} 5$ zu zeigen.

Es ist

$$\begin{aligned}\mathrm{Cl}(\mathbf{Z}[\alpha]) &= \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\alpha]) \text{ mit } |\mathbf{Z}[\alpha]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\sqrt{-23})}\,\} \\ &= \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\alpha]) \text{ mit } |\mathbf{Z}[\alpha]/\mathfrak{a}| \leqslant 3\,\}\,;\end{aligned}$$

cf. Satz 118.(1).

Für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\alpha])$ mit $\mathfrak{p} \cap \mathbf{Z} = (p)$, wobei $p \in \mathbf{Z}_{>0}$ prim, ist $\mathbf{Z}[\alpha]/\mathfrak{p}$ eine Körpererweiterung von $\mathbf{Z}/(p) = \mathbf{F}_p$ und also $|\mathbf{Z}[\alpha]/\mathfrak{p}| \geqslant p$; cf. Aufgabe 43.(1). Für die Entscheidung, welche $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\alpha])$ die Bedingung $|\mathbf{Z}[\alpha]/\mathfrak{p}| \leqslant 3$ erfüllen, müssen also nur die in der Primidealfaktorzerlegung von (2) und von (3) in $\mathbf{Z}[\alpha]$ auftretenden Primideale herangezogen werden.

Es ist $\mu_{\alpha,\mathbf{Q}}(X) = X^2 - X + 6$. Wir verwenden die Methode aus der Lösung zu Aufgabe 30.(2).

Es ist $X^2 - X + 6 \equiv_2 X(X-1)$ die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_2[X]$. Das gibt in $\mathbf{Z}[\alpha]$ die Primidealfaktorzerlegung

$$(2) \;=\; \underbrace{(\alpha,\,2)}_{=:\,\mathfrak{p}_{1,1}}\underbrace{(\alpha-1,\,2)}_{=:\,\mathfrak{p}_{1,2}}\,.$$

Es folgt $|\mathbf{Z}[\alpha]/\mathfrak{p}_{1,1}| = 2^1$ und $|\mathbf{Z}[\alpha]/\mathfrak{p}_{1,2}| = 2^1$ dank Aufgabe 43.(2).

Es ist $X^2 - X + 6 \equiv_3 X(X-1)$ die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_3[X]$. Das gibt in $\mathbf{Z}[\alpha]$ die Primidealfaktorzerlegung

$$(3) \;=\; \underbrace{(\alpha,\,3)}_{=:\,\mathfrak{p}_{2,1}}\underbrace{(\alpha-1,\,3)}_{=:\,\mathfrak{p}_{2,2}}\,.$$

Es folgt $|\mathbf{Z}[\alpha]/\mathfrak{p}_{2,1}| = 3^1$ und $|\mathbf{Z}[\alpha]/\mathfrak{p}_{2,2}| = 3^1$ dank Aufgabe 43.(2).

Unter Verwendung von Bemerkung 92 wird demnach

$$\mathrm{Cl}(\mathbf{Z}[\alpha]) \;=\; \{[(1)],\,[\mathfrak{p}_{1,1}],\,[\mathfrak{p}_{1,2}],\,[\mathfrak{p}_{2,1}],\,[\mathfrak{p}_{2,2}]\}$$

und somit in der Tat $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \leqslant 5$; cf. Satz 63.(1).

Ad (2). Wir haben, in Standardbezeichnungen, die Minkowskischranke

$$\xi_{\mathbf{Q}(\sqrt{-47})} \;=\; \frac{k!}{k^k}\cdot\left(\frac{4}{\pi}\right)^s\cdot|\Delta_{\mathbf{Q}(\sqrt{-47})}|^{1/2} \;=\; \frac{1}{2}\cdot\frac{4}{\pi}\cdot|-47|^{1/2} \;\approx\; 4{,}3644\,;$$

cf. Definition 115, Aufgabe 16.(1).

Sei $\alpha := \frac{1}{2}(1+\sqrt{-47})$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{-47})} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Wir haben also $\mathrm{Cl}(\mathbf{Z}[\alpha]) \overset{!}{\simeq} \mathrm{C}_5$ zu zeigen. Dank Aufgabe 36.(2) gibt es ein Element der Ordnung 5 in $\mathrm{Cl}(\mathbf{Z}[\alpha])$. Also genügt es, $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \overset{!}{\leqslant} 5$ zu zeigen. Da 5 ein Teiler von $|\mathrm{Cl}(\mathbf{Z}[\alpha])|$ ist, genügt es hierfür, $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \overset{!}{\leqslant} 9$ zu zeigen.

Es ist

$$\begin{aligned}\mathrm{Cl}(\mathbf{Z}[\alpha]) &= \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\alpha]) \text{ mit } |\mathbf{Z}[\alpha]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\sqrt{-47})}\,\} \\ &= \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\alpha]) \text{ mit } |\mathbf{Z}[\alpha]/\mathfrak{a}| \leqslant 4\,\}\,;\end{aligned}$$

cf. Satz 118.(1).

Für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\alpha])$ mit $\mathfrak{p} \cap \mathbf{Z} = (p)$, wobei $p \in \mathbf{Z}_{>0}$ prim, ist $\mathbf{Z}[\alpha]/\mathfrak{p}$ eine Körpererweiterung von $\mathbf{Z}/(p) = \mathbf{F}_p$ und also $|\mathbf{Z}[\alpha]/\mathfrak{p}| \geqslant p$; cf. Aufgabe 43.(1). Für die Entscheidung, welche $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\alpha])$

die Bedingung $|\mathbf{Z}[\alpha]/\mathfrak{p}| \leqslant 4$ erfüllen, müssen also nur die in der Primidealfaktorzerlegung von (2) und von (3) in $\mathbf{Z}[\alpha]$ auftretenden Primideale herangezogen werden.

Es ist $\mu_{\alpha,\mathbf{Q}}(X) = X^2 - X + 12$. Wir verwenden die Methode aus der Lösung zu Aufgabe 30.(2).

Es ist $X^2 - X + 12 \equiv_2 X(X-1)$ die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_2[X]$. Das gibt in $\mathbf{Z}[\alpha]$ die Primidealfaktorzerlegung

$$(2) \;=\; \underbrace{(\alpha,\, 2)}_{=:\,\mathfrak{p}_{1,1}} \underbrace{(\alpha - 1,\, 2)}_{=:\,\mathfrak{p}_{1,2}} \;.$$

Es folgt $|\mathbf{Z}[\alpha]/\mathfrak{p}_{1,1}| = 2^1$ und $|\mathbf{Z}[\alpha]/\mathfrak{p}_{1,2}| = 2^1$ dank Aufgabe 43.(2).

Es ist $X^2 - X + 12 \equiv_3 X(X-1)$ die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_3[X]$. Das gibt in $\mathbf{Z}[\alpha]$ die Primidealfaktorzerlegung

$$(3) \;=\; \underbrace{(\alpha,\, 3)}_{=:\,\mathfrak{p}_{2,1}} \underbrace{(\alpha - 1,\, 3)}_{=:\,\mathfrak{p}_{2,2}} \;.$$

Es folgt $|\mathbf{Z}[\alpha]/\mathfrak{p}_{2,1}| = 3^1$ und $|\mathbf{Z}[\alpha]/\mathfrak{p}_{2,2}| = 3^1$ dank Aufgabe 43.(2).

Unter Verwendung von Bemerkung 92 wird demnach

$$\mathrm{Cl}(\mathbf{Z}[\alpha]) \;=\; \{[(1)],\, [\mathfrak{p}_{1,1}],\, [\mathfrak{p}_{1,2}],\, [\mathfrak{p}_{2,1}],\, [\mathfrak{p}_{2,2}],\, [\mathfrak{p}_{1,1}^2],\, [\mathfrak{p}_{1,2}^2],\, [\mathfrak{p}_{1,1}\mathfrak{p}_{1,2}]\}$$

und somit in der Tat $|\mathrm{Cl}(\mathbf{Z}[\alpha])| \leqslant 8 \leqslant 9$; cf. Satz 63.(1).

Aufgabe 48

Wir wollen zeigen, daß $\mathbf{Z}[\sqrt[3]{2}]$ ein Hauptidealbereich ist. Es ist $k = 3$, $r = 1$ und $s = 1$; cf. Aufgabe 7.

Schreibe $\delta := \sqrt[3]{2}$. Wir haben, in Standardbezeichnungen, die Minkowskischranke

$$\xi_{\mathbf{Q}(\delta)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\delta)}|^{1/2} \;=\; \frac{2}{9} \cdot \frac{4}{\pi} \cdot |-108|^{1/2} \;\approx 2{,}9404\;;$$

cf. Definition 115, Aufgabe 16.(1).

Es ist $\mathcal{O}_{\mathbf{Q}(\delta)} = \mathbf{Z}[\delta]$; cf. Aufgabe 19.(2). Wir haben $|\mathrm{Cl}(\mathbf{Z}[\delta])| \stackrel{!}{=} 1$ zu zeigen; cf. Bemerkung 69.(1).

Es ist

$$\begin{aligned} \mathrm{Cl}(\mathbf{Z}[\delta]) \;&=\; \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\delta]) \text{ mit } |\mathbf{Z}[\delta]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\delta)}\,\} \\ &=\; \{\,[\mathfrak{a}] \,:\, \mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\delta]) \text{ mit } |\mathbf{Z}[\delta]/\mathfrak{a}| \leqslant 2\,\}\;; \end{aligned}$$

cf. Satz 118.(1).

Dank Bemerkung 92 genügt es zu zeigen, daß alle $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\delta])$ mit $|\mathbf{Z}[\delta]/\mathfrak{p}| \leqslant 2$ Hauptideale sind.

Für $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\delta])$ mit $\mathfrak{p} \cap \mathbf{Z} = (p)$, wobei $p \in \mathbf{Z}_{>0}$ prim, ist $\mathbf{Z}[\delta]/\mathfrak{p}$ eine Körpererweiterung von $\mathbf{Z}/(p) = \mathbf{F}_p$ und also $|\mathbf{Z}[\delta]/\mathfrak{p}| \geqslant p$; cf. Aufgabe 43.(1). Für die Entscheidung, welche $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\delta])$ die Bedingung $|\mathbf{Z}[\delta]/\mathfrak{p}| \leqslant 2$ erfüllen, müssen also nur die in der Primidealfaktorzerlegung von (2) in $\mathbf{Z}[\delta]$ auftretenden Primideale herangezogen und als Hauptideale nachgewiesen werden.

Es ist $\mu_{\delta,\mathbf{Q}}(X) = X^3 - 2$; cf. Lösung zu Aufgabe 7. Wir verwenden die Methode aus der Lösung zu Aufgabe 30.(2).

Es ist $X^3 - 2 \equiv_2 X^3$ die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_2[X]$. Das gibt in $\mathbf{Z}[\delta]$ die Primidealfaktorzerlegung

$$(2) \;=\; (\delta, 2)^3 \;=\; (\delta)^3\;;$$

beachte $2 = \delta \cdot \delta^2$.

Das einzige zu betrachtende Primideal ist also ein Hauptideal, namentlich (δ).

Aufgabe 49

Ad (1). Nach Satz 118.(1) können wir ein $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathcal{O}_K)$ mit $|\mathcal{O}_K/\mathfrak{a}| \leqslant \xi_K$ so wählen, daß $[(1)] = [\mathfrak{a}]$ ist. Es folgt

$$1 \;\leqslant\; |\mathcal{O}_K/\mathfrak{a}| \;\leqslant\; \xi_K \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_K|^{1/2}\,,$$

und also

$$\left(\frac{\pi}{4}\right)^{2s} \cdot \left(\frac{k^k}{k!}\right)^2 \;\leqslant\; |\Delta_K|$$

Ad (2). Wir wollen zeigen, daß $|\Delta_K| = 1$ nur für $K = \mathbf{Q}$ gilt. Wegen $2s \leqslant k$ genügt es dazu zu zeigen, daß für $k \geqslant 2$ sich

$$f(k) \;:=\; \left(\frac{\pi}{4}\right)^k \cdot \left(\frac{k^k}{k!}\right)^2 \;\overset{!}{>}\; 1$$

ergibt.

Für $k = 2$ trifft dies zu, da $f(2) = (\frac{\pi}{4})^2 \cdot 2^2 = (\frac{\pi}{2})^2 > 1$.

Ferner ist für $k \geqslant 2$

$$\frac{f(k+1)}{f(k)} \;=\; \frac{\pi}{4} \cdot \left(\frac{(k+1)^{k+1} \cdot k!}{(k+1)! \cdot k^k}\right)^2 \;=\; \frac{\pi}{4} \cdot \left(1 + \frac{1}{k}\right)^{2k}$$

Es wächst $\left(1 + \frac{1}{k}\right)^k$ monoton mit $k \geqslant 1$; dies ist aus der Analysis bekannt, wir erinnern unten an ein Argument. Also ist

$$\frac{f(k+1)}{f(k)} \;\geqslant\; \frac{f(3)}{f(2)} \;=\; \frac{\pi}{4} \cdot \left(1 + \frac{1}{2}\right)^4 \;>\; \frac{3^5}{2^6} \;>\; 1$$

Also ist $f(k)$ monoton wachsend mit $k \geqslant 2$, und daher $f(k) \geqslant f(2) > 1$ für $k \geqslant 2$.

Wir erinnern nun noch an das monotone Wachstum von $\left(1 + \frac{1}{k}\right)^k$. Für $x \in \mathbf{R}_{\geqslant 1}$ wird

$$\left(1 + \frac{1}{x}\right)^x \;=\; \exp(\ln(1 + \frac{1}{x}) \cdot x) \;=\; \exp((\ln(x+1) - \ln(x)) \cdot x)\,.$$

Wir haben für $x \in \mathbf{R}_{\geqslant 1}$

$$0 \;\overset{!}{<}\; ((\ln(x+1) - \ln(x)) \cdot x)' \;=\; (\frac{1}{x+1} - \frac{1}{x}) \cdot x + \ln(x+1) - \ln(x) \;=\; -\frac{1}{x+1} + \ln(x+1) - \ln(x)$$

zu zeigen.

Nun ist zum einen $\lim_{x\to\infty} -\frac{1}{x+1} + \ln(x+1) - \ln(x) \;=\; -\lim_{x\to\infty} \frac{1}{x+1} + \lim_{x\to\infty} \ln(1 + \frac{1}{x}) = 0$, zum anderen ist $-\frac{1}{x+1} + \ln(x+1) - \ln(x)$ streng monoton fallend in $x \in \mathbf{R}_{\geqslant 1}$ wegen

$$(-\frac{1}{x+1} + \ln(x+1) - \ln(x))' \;=\; \frac{1}{(x+1)^2} + \frac{1}{x+1} - \frac{1}{x} \;=\; \frac{x + (x+1)x - (x+1)^2}{(x+1)^2 x} \;=\; -\frac{1}{(x+1)^2 x} \;<\; 0\,.$$

Somit kann für kein $x \in \mathbf{R}_{\geqslant 1}$ der Wert $-\frac{1}{x+1} + \ln(x+1) - \ln(x) \leqslant 0$ sein.

Ad (3). Wegen $2s \leqslant k$ ist stets $5^{-k}|\Delta_K| \geqslant 5^{-k} \left(\frac{k^k}{k!}\right)^2 \left(\frac{\pi}{4}\right)^k$; cf. (1). Mit Stirling ergibt sich weiter, daß es für jedes $\varepsilon \in \mathbf{R}$ mit $0 < \varepsilon < 1$ ein $M \in \mathbf{Z}_{\geqslant 1}$ so gibt, daß für $n \geqslant M$

$$5^{-n} \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n \geqslant (1 - \varepsilon) \left(\frac{\mathrm{e}^2\pi}{20}\right)^n (2\pi n)^{-1} \;\geqslant\; (1 - \varepsilon)(10/9)^n (2\pi n)^{-1}$$

ist. Wir wählen uns e.g. $\varepsilon = 1/2$. Die rechte Seite geht mit $n \to \infty$ gegen $+\infty$, also auch die linke. Durch Einsetzen der Definition der bestimmten Divergenz folgt das Ergebnis.

Aufgabe 50

Ad (1). Zeigen wir die Wohldefiniertheit. Seien $\mathfrak{h}$, $\tilde{\mathfrak{h}} \in \underline{\text{Ideale}}^\times(B)$ mit $[\mathfrak{h}] = [\tilde{\mathfrak{h}}]$ gegeben. Dann gibt es ein $y \in L^\times$ mit $(y)\mathfrak{h} = \tilde{\mathfrak{h}}$. Es folgt

$$\mathrm{N}_{L|K}(\tilde{\mathfrak{h}}) \;=\; \mathrm{N}_{L|K}(\,(y)\mathfrak{h}\,) \overset{\text{L. 88}}{=} \mathrm{N}_{L|K}(\,(y)\,)\,\mathrm{N}_{L|K}(\mathfrak{h}) \overset{\text{B. 86.(3)}}{=} (\,\mathrm{N}_{L|K}(y)\,)\,\mathrm{N}_{L|K}(\mathfrak{h})\;,$$

und damit $[\mathrm{N}_{L|K}(\tilde{\mathfrak{h}})] = [\mathrm{N}_{L|K}(\mathfrak{h})]$.

Sodann ist für $\mathfrak{h}$, $\mathfrak{h}' \in \underline{\text{Ideale}}^\times(B)$ auch

$$\begin{aligned}
\mathrm{N}_{L|K}([\mathfrak{h}][\mathfrak{h}']) &= \mathrm{N}_{L|K}([\mathfrak{h}\mathfrak{h}']) \\
&= [\mathrm{N}_{L|K}(\mathfrak{h}\mathfrak{h}')] \\
&\overset{\text{L. 88}}{=} [\mathrm{N}_{L|K}(\mathfrak{h})\,\mathrm{N}_{L|K}(\mathfrak{h}')] \\
&= [\mathrm{N}_{L|K}(\mathfrak{h})][\mathrm{N}_{L|K}(\mathfrak{h}')] \\
&= \mathrm{N}_{L|K}([\mathfrak{h}])]\,\mathrm{N}_{L|K}([\mathfrak{h}'])\;,
\end{aligned}$$

und daher $\mathrm{N}_{L|K}$ auf den Klassengruppen ein Gruppenmorphismus.

Ad (2). Zeigen wir die Wohldefiniertheit. Seien $\mathfrak{g}$, $\tilde{\mathfrak{g}} \in \underline{\text{Ideale}}^\times(A)$ mit $[\mathfrak{g}] = [\tilde{\mathfrak{g}}]$ gegeben. Dann gibt es ein $x \in K^\times$ mit $(x)\mathfrak{g} = \tilde{\mathfrak{g}}$. Es folgt

$$B\tilde{\mathfrak{g}} \;=\; B(x)\mathfrak{g} \;=\; BAx\mathfrak{g} \;=\; Bx\mathfrak{g} \;=\; BxB\mathfrak{g} \;=\; (x)B\mathfrak{g}\;,$$

und damit $[B\tilde{\mathfrak{g}}] = [B\mathfrak{g}]$.

Sodann ist für $\mathfrak{g}$, $\mathfrak{g}' \in \underline{\text{Ideale}}^\times(A)$ auch

$$\mathrm{ind}_{L|K}([\mathfrak{g}])\mathrm{ind}_{L|K}([\mathfrak{g}']) \;=\; [B\mathfrak{g}][B\mathfrak{g}'] \;=\; [B\mathfrak{g}B\mathfrak{g}'] \;=\; [B\mathfrak{g}\mathfrak{g}'] \;=\; \mathrm{ind}_{L|K}([\mathfrak{g}\mathfrak{g}'])\;.$$

$\mathrm{ind}_{L|K}$ auf den Klassengruppen also ein Gruppenmorphismus.

Ad (3). Für $\mathfrak{g} \in \underline{\text{Ideale}}^\times(A)$ ist

$$\mathrm{N}_{L|K}(\mathrm{ind}_{L|K}([\mathfrak{g}])) \;=\; \mathrm{N}_{L|K}([B\mathfrak{g}]) \;=\; [\mathrm{N}_{L|K}(B\mathfrak{g})] \overset{\text{A. 34.(3)}}{=} [\mathfrak{g}^\ell] = [\mathfrak{g}]^\ell\;.$$

Für $m \in \mathbf{Z}$ betrachten wir den Gruppenmorphismus $\varepsilon_m : \mathrm{Cl}(A) \to \mathrm{Cl}(A)$, $[\mathfrak{g}] \mapsto [\mathfrak{g}]^m$, welcher auf jeder multiplikativ geschriebenen abelschen Gruppe in dieser Weise definiert werden kann. Es ist $\mathrm{N}_{L|K} \circ \mathrm{ind}_{L|K} = \varepsilon_\ell$.

Schreibe $c := |\mathrm{Cl}(A)|$. Für $[\mathfrak{g}] \in \mathrm{Cl}(A)$ ist $[\mathfrak{g}]^c = [(1)]$; cf. **[5,** Aufgabe 11.(1.c)].

Seien c und ℓ als teilerfremd vorausgesetzt. Wähle s, $t \in \mathbf{Z}$ so, daß $sc+t\ell = 1$ ist. Dann wird $\varepsilon_t(\varepsilon_\ell([\mathfrak{g}])) = [\mathfrak{g}]^{t\ell} = [\mathfrak{g}]^{sc+t\ell} = [\mathfrak{g}]$ für $[\mathfrak{g}] \in \mathrm{Cl}(A)$ und also $\varepsilon_t \circ \varepsilon_\ell = \mathrm{id}_{\mathrm{Cl}(A)}$. Genauso ist auch $\varepsilon_\ell \circ \varepsilon_t = \mathrm{id}_{\mathrm{Cl}(A)}$. Somit ist ε_ℓ ein Isomorphismus.

Aus ε_ℓ bijektiv und aus $\mathrm{N}_{L|K} \circ \mathrm{ind}_{L|K} = \varepsilon_\ell$ folgt nun $\mathrm{ind}_{L|K}$ injektiv und $\mathrm{N}_{L|K}$ surjektiv auf den Klassengruppen.

Aufgabe 51

Ad (1). Wegen $b^m - a = 0$ ist $b \in B$.

Es genügt, $B\mathfrak{a} \stackrel{!}{=} (b) \subseteq B$ zu zeigen. Es genügt, $\mathrm{v}_\mathfrak{p}(b) \stackrel{!}{=} \mathrm{v}_\mathfrak{p}(\mathfrak{a})$ für $\mathfrak{p} \in \mathrm{Ideale}^\times_{\mathrm{prim}}(B)$ zu zeigen; cf. Lemmata 54 und 65. Es genügt, $m\,\mathrm{v}_\mathfrak{p}(b) \stackrel{!}{=} m\,\mathrm{v}_\mathfrak{p}(\mathfrak{a})$ zu zeigen.

In der Tat ist $m\,\mathrm{v}_\mathfrak{p}(b) = \mathrm{v}_\mathfrak{p}(b^m) = \mathrm{v}_\mathfrak{p}(a) = \mathrm{v}_\mathfrak{p}(\mathfrak{a}^m) = m\,\mathrm{v}_\mathfrak{p}(\mathfrak{a})$.

Man sagt, $\mathfrak{a}$ *kapituliert* in B.

Ad (2). Es ist $\mathrm{Cl}(\mathcal{O}_K)$ eine endliche Gruppe; cf. Satz 118. Wähle $n \geqslant 0$ und $\mathfrak{a}_i \in \mathrm{Ideale}^\times(\mathcal{O}_K)$ für $i \in [1,n]$ so, daß $\mathrm{Cl}(K) = \langle\!\langle\, [\mathfrak{a}_i] \,:\, i \in [1,n] \,\rangle\!\rangle$ ist. Schreibe $m_i := |\langle\!\langle [\mathfrak{a}_i] \rangle\!\rangle|$ für $i \in [1,n]$.

Es genügt, eine Zahlkörpererweiterung $L|K$ so zu finden, daß $\mathrm{ind}_{L|K}([\mathfrak{a}_i]) = [(1)]$ ist für $i \in [1,n]$, da $\mathrm{ind}_{L|K}$ ein Gruppenmorphismus ist; cf. Aufgabe 50.(2).

Sei nun M ein Zerfällungskörper von $\prod_{i\in[1,n]}(X^{m_i} - a_i) \in K[X]$. Wähle $b_i \in M$ mit $b_i^{m_i} = a_i$ für $i \in [1,n]$. Sei $L := K(b_1, \ldots, b_n)$. Es ist $L|K$ eine endliche Körpererweiterung. Da für $i \in [1,n]$ nach Konstruktion $\mathrm{ind}_{L|K} = \mathrm{ind}_{L|K(b_i)} \circ \mathrm{ind}_{K(b_i)|K}$ und $\mathrm{ind}_{K(b_i)|K}([\mathfrak{a}_i]) \stackrel{(1)}{=} [(1)]$ ist, ist in der Tat stets $\mathrm{ind}_{L|K}([\mathfrak{a}_i]) = [(1)]$.

Ad (3). Es ist $[(2, 1+\sqrt{-5})]$ ein Erzeuger der Gruppe $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-5})})$ von Ordnung 2 und es ist $(2, 1+\sqrt{-5})^2 = (2)$; cf. Beispiel 119. Dank (2) ist also

$$\mathrm{ind}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})|\mathbf{Q}(\sqrt{-5})}$$

trivial und wir können $L = \mathbf{Q}(\sqrt{-5}, \sqrt{2})$ wählen.

Betrachte $\mathfrak{a} = (2, 1+\sqrt{-5})$, welches in $\mathcal{O}_K$ kein Hauptideal ist; cf. Aufgabe 6.(4). Wähle $b := \sqrt{2} \in \mathcal{O}_L$.

Wir wollen in $\mathcal{O}_L = \mathcal{O}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})}$ die Idealgleichheit $(2, 1+\sqrt{-5}) \stackrel{!}{=} (\sqrt{2})$ zeigen.

Hierbei gilt $\subseteq$, da

$$\begin{aligned} 2 &= \sqrt{2}\cdot\sqrt{2} \\ 1+\sqrt{-5} &= \sqrt{2}\cdot\tfrac{\sqrt{2}}{2}(1+\sqrt{-5}) \,, \end{aligned}$$

ist und da letzterer Faktor Minimalpolynom $X^2 + (2-\sqrt{-5})$ über $\mathbf{Z}[\sqrt{-5}]$ hat, sich also in $\mathcal{O}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})}$ befindet.

Nun gilt

$$\begin{aligned} \mathrm{N}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})|\mathbf{Q}}(\,(2, 1+\sqrt{-5})\,) &= \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(\mathrm{N}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})|\mathbf{Q}(\sqrt{-5})}(\,(2, 1+\sqrt{-5})\,)) \\ &= \mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(\,(2, 1+\sqrt{-5})\,)^2 \\ &= (4)\,; \end{aligned}$$

cf. Aufgabe 34.(2, 3), Beispiel 93.

Analog gilt

$$\begin{aligned} \mathrm{N}_{\mathbf{Q}(\sqrt{-5},\sqrt{2})|\mathbf{Q}}(\,(\sqrt{2})\,) &= \mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(\mathrm{N}_{\mathbf{Q}(\sqrt{2},\sqrt{2})|\mathbf{Q}(\sqrt{-5})}(\,(\sqrt{2})\,)) \\ &= \mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(\,(\sqrt{2})\,)^2 \\ &= \mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(\,(2)\,) \\ &= (4)\,; \end{aligned}$$

cf. Aufgabe 34.(2, 3), Lemma 88, Bemerkung 86.(3).

Daher ist die Norm des Ideals $(2, 1+\sqrt{-5})(\sqrt{2})^{-1}$ gleich (1), i.e. es ist $(2, 1+\sqrt{-5})(\sqrt{2})^{-1} = (1)$; cf. Lemma 91. Somit ist die Gleichheit der fraglichen Ideale vollends nachgewiesen.

Aufgabe 52

Ad (1). Es ist $(s\circ r-\mathrm{id}_M)(m)$ im Kern von r, da $r(s(r(m))-m=0$ ist. Setze $t(m):=m'$, wobei $m'\in M'$ das eindeutige Element mit $i(m')=(s\circ r-\mathrm{id}_M)(m)$ ist.

Es ist t eine R-lineare Abbildung. Denn für $m,\,\tilde m\,\in\,M$ und $x,\,\tilde x\,\in\,R$ ist $i(xt(m)+\tilde xt(\tilde m))=xi(t(m))+\tilde xi(t(\tilde m))=x(s\circ r-\mathrm{id}_M)(m)+\tilde x(s\circ r-\mathrm{id}_M)(\tilde m)\;=\;(s\circ r-\mathrm{id}_M)(xm+\tilde x\tilde m)$ und also $xt(m)+\tilde xt(\tilde m)=t(xm+\tilde x\tilde m)$.

Für $m'\in M'$ ist $i(t(i(m')))=(s\circ r-\mathrm{id}_M)(i(m'))=i(m')$ und also $t(i(m'))=m'$. Mithin ist $t\circ i=\mathrm{id}_{M'}$.

Merken wir noch an, daß für $m''\in M''$ sich $i(t(s(m'')))=(s\circ r-\mathrm{id}_M)(s(m''))=s(m'')-s(m'')=0$ und also $t(s(m''))=0$ ergibt. Mithin ist $t\circ s=0$.

Wir haben daraus die R-linearen Abbildungen

$$\begin{array}{rcccc} M & \longleftrightarrow & M' & \oplus & M'' \\ m & \overset{f}{\longmapsto} & (t(m) & , & r(m)) \\ i(m')+s(m'') & \overset{g}{\longmapsfrom} & (m' & , & m'')\,. \end{array}$$

Insbesondere ist $g(\,(m',0)\,)=i(m')$ für $m'\in M'$.

Für $m\in M$ ist $g(f(m))=i(t(m))+s(r(m))=(s\circ r-\mathrm{id}_M)(m)+s(r(m))=m$.

Für $(m',m'')\,\in\,M'\oplus M''$ ist $f(g(\,(m',m'')\,))\;=\;(t(i(m')+s(m'')),r(i(m')+s(m'')))\;=\;(t(i(m'))+t(s(m'')),r(i(m'))+r(s(m'')))=(m',m'')$.

Also sind f und g sich gegenseitig invertierende Isomorphismen von R-Moduln.

Ad (2). Gemäß (1) genügt es zu zeigen, daß es eine R-lineare Abbildung $M''\overset{s}{\to}M$ mit $r\circ s=\mathrm{id}_{M''}$ existiert.

Sei $\mathrm{e}_i\in R^{\oplus n}$ der i-te Standardbasisvektor, der im i-ten Tupeleintrag eine 1 und sonst 0 stehen hat; sei $p_i:R^{\oplus n}\to R$ die Projektionsabbildung auf den i-ten Tupeleintrag; beides für $i\in[1,n]$. Wähle einen Isomorphismus $h:R^{\oplus n}\overset{\sim}{\to}M''$.

Wähle für alle $m''\in M''$ ein $\sigma(m'')\in M$ mit $r(\sigma(m''))$, möglich, da r surjektiv ist.

> Beachte, daß σ nicht notwendig R-linear ist.

Setze

$$\begin{array}{ccc} M'' & \overset{s}{\longrightarrow} & M \\ m'' & \longmapsto & \sum_{i\in[1,n]}p_i(h^{-1}(m''))\sigma(h(\mathrm{e}_i))\,. \end{array}$$

Da h und p_i für $i\in[1,n]$ alle R-linear sind, ist auch s eine R-lineare Abbildung.

Für $m''\in M''$ ist ferner

$$\begin{array}{rcl} r(s(m'')) & = & r\big(\sum_{i\in[1,n]}p_i(h^{-1}(m''))\sigma(h(\mathrm{e}_i))\big) \\ & = & \sum_{i\in[1,n]}p_i(h^{-1}(m''))r(\sigma(h(\mathrm{e}_i))) \\ & = & \sum_{i\in[1,n]}p_i(h^{-1}(m''))h(\mathrm{e}_i) \\ & = & h\big(\sum_{i\in[1,n]}p_i(h^{-1}(m''))\mathrm{e}_i\big) \\ & = & h\big((p_i(h^{-1}(m'')))_i\big) \\ & = & h\big(h^{-1}(m'')\big) \\ & = & m''\,. \end{array}$$

Mithin ist $r\circ s=\mathrm{id}_{M''}$.

Aufgabe 53

Ad (1). Es ist $\mu(\mathbf{Q}(\sqrt{d})) = \{-1,+1\}$, da $\mathbf{Q}(\sqrt{d}) \subseteq \mathbf{R}$, da alle Elemente von $\mu(\mathbf{Q}(\sqrt{d}))$ Betrag 1 in $\mathbf{C}$ haben müssen und da in $\mathbf{R}$ nur die beiden Elemente -1 und $+1$ Betrag 1 haben.

Es ist $r := |\mathrm{Einb}_{\mathbf{R}}(\mathbf{Q}(\sqrt{d}))| = 2$ und $s := |\mathrm{Einb}_{\mathbf{C}}(\mathbf{Q}(\sqrt{d}))| = 0$, folglich $r+s-1 = 1$. Nach Dirichlet gibt es also einen Gruppenmorphismus

$$\mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})}) \xleftarrow{\sim} \{-1,+1\} \times \mathbf{Z}\,,$$

der $(x,0)$ auf x schickt für $x \in \{-1,+1\}$; cf. Satz 126.

Beachte, daß für (x,a), $(x',a') \in \{-1,+1\} \times \mathbf{Z}$ die Multiplikation durch $(x,a)(\tilde{x},\tilde{a}) = (x\tilde{x}, a+\tilde{a})$ gegeben ist.

In $\{-1,+1\} \times \mathbf{Z}$ gibt es genau 4 Elemente (y,b) mit der Eigenschaft, daß für alle $(x,a) \in \{-1,+1\} \times \mathbf{Z}$ genau ein $m \in \mathbf{Z}$ existiert mit $(x,a) \in \{(-1,0)(y,b)^m, (+1,0)(y,b)^m\}$, nämlich $(1,1)$, $(1,-1)$, $(-1,1)$ und $(-1,-1)$. Ist (y_0,b_0) eines dieser Elemente, dann wird

$$\begin{aligned} & \{\,(1,1)\,,\,(1,-1)\,,\,(-1,1)\,,\,(-1,-1)\,\} \\ = \;& \{\,(y_0\,,\,b_0)\,,\,(y_0\,,\,-b_0)\,,\,(-y_0\,,\,b_0)\,,\,(-y_0\,,\,-b_0)\,\} \\ = \;& \{\,(y_0\,,\,b_0)\,,\,(y_0\,,\,b_0)^{-1}\,,\,(-1,0)(y_0\,,\,b_0)\,,\,(-1,0)(y_0\,,\,b_0)\,\}\,. \end{aligned}$$

Isomorph übertragen auf $\mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})})$ bedeutet dies, daß es in $\mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})})$ genau 4 Elemente u gibt mit der Eigenschaft, daß für alle $v \in \mathrm{U}(\mathcal{O}_{\mathbf{Q}(\sqrt{d})})$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u^m, +u^m\}$ existiert. Sei u_0 ein solches Element. Dann sind alle diese Elemente gegeben durch

$$\{\,u_0\,,\,u_0^{-1}\,,\,-u_0\,,\,-u_0^{-1}\,\} \;\subseteq\; \mathbf{R} \smallsetminus \{0,-1,+1\}\,.$$

Das maximale Element dieser Menge ist zugleich das einzige Element dieser Menge > 1.

Ad (2).

Fall $d = 2$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{2})} = \mathbf{Z}[\sqrt{2}]$; cf. Aufgabe 3.

Ist $u = a + b\sqrt{2} \in \mathrm{U}(\mathbf{Z}[\sqrt{2}]) \cap \mathbf{R}_{>1}$ mit $a,\, b \in \mathbf{Z}$ gegeben wie in (1), dann ist $\mathrm{N}_{\mathbf{Q}(\sqrt{2})|\mathbf{Q}}(u) = a^2 - 2b^2 \in \{-1,+1\}$. Ferner ist $b \neq 0$, denn $b = 0$ hieße $u = a \in \mathrm{U}(\mathbf{Z}) = \{-1,+1\}$, was nicht der Fall ist.

Es ist

$$\{\,u\,,\,u^{-1}\,,\,-u\,,\,-u^{-1}\,\} \;=\; \{\,a+b\sqrt{2}\,,\,a-b\sqrt{2}\,,\,-a+b\sqrt{2}\,,\,-a-b\sqrt{2}\,,\;\}\,.$$

Da u das maximale Element dieser Menge ist, folgt $a \geqslant 0$ und $b \geqslant 1$.

Es gibt in $\mathrm{U}(\mathbf{Z}[\sqrt{2}]) \cap \mathbf{R}_{>1}$ kein kleineres Element als u, da jedes dieser Elemente eine Potenz von u ist.

Nun ist $a^2 = \pm 1 + 2b^2$, was für jedes dieser Vorzeichen separat monoton in b wächst. Wir suchen also die erste Quadratzahl a^2 in der Folge

$$-1+2\cdot 1^2,\; +1+2\cdot 1^2,\; -1+2\cdot 2^2,\; +1+2\cdot 2^2,\; \ldots$$

Dies führt uns auf $a^2 = -1 + 2\cdot 1^2 = 1$ und auf $u = 1+\sqrt{2}$.

Fall $d = 3$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{3})} = \mathbf{Z}[\sqrt{3}]$; cf. Aufgabe 3.

Ist $u = a + b\sqrt{3} \in \mathrm{U}(\mathbf{Z}[\sqrt{3}]) \cap \mathbf{R}_{>1}$ mit $a,\, b \in \mathbf{Z}$ gegeben wie in (1), dann ist $\mathrm{N}_{\mathbf{Q}(\sqrt{3})|\mathbf{Q}}(u) = a^2 - 3b^2 \in \{-1,+1\}$. Ferner ist $b \neq 0$, denn $b = 0$ hieße $u = a \in \mathrm{U}(\mathbf{Z}) = \{-1,+1\}$, was nicht der Fall ist.

Es ist

$$\{\,u\,,\,u^{-1}\,,\,-u\,,\,-u^{-1}\,\} \;=\; \{\,a+b\sqrt{3}\,,\,a-b\sqrt{3}\,,\,-a+b\sqrt{3}\,,\,-a-b\sqrt{3}\,,\;\}\,.$$

Da u das maximale Element dieser Menge ist, folgt $a \geqslant 0$ und $b \geqslant 1$.

Es gibt in $\mathrm{U}(\mathbf{Z}[\sqrt{3}]) \cap \mathbf{R}_{>1}$ kein kleineres Element als u, da jedes dieser Elemente eine Potenz von u ist.

Nun ist $a^2 = \pm 1 + 3b^2$, was für jedes dieser Vorzeichen separat monoton in b wächst. Wir suchen also die erste Quadratzahl a^2 in der Folge

$$-1 + 3 \cdot 1^2,\ +1 + 3 \cdot 1^2,\ -1 + 3 \cdot 2^2,\ +1 + 3 \cdot 2^2,\ \ldots$$

Dies führt uns auf $a^2 = 1 + 3 \cdot 1^2 = 4$ und auf $u = 2 + \sqrt{3}$.

Fall $d = 5$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{5})]$; cf. Aufgabe 3. Schreibe $\alpha := \frac{1}{2}(1 + \sqrt{5})$.

I.e. es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \{\, \frac{1}{2}(a + b\sqrt{5}) \,:\, a, b \in \mathbf{Z},\ a \equiv_2 b \,\}$.

Ist $u = \frac{1}{2}(a + b\sqrt{5}) \in \mathrm{U}(\mathbf{Z}[\alpha]) \cap \mathbf{R}_{>1}$ mit $a, b \in \mathbf{Z}$ und $a \equiv_2 b$ gegeben wie in (1), dann ist $\mathrm{N}_{\mathbf{Q}(\alpha)|\mathbf{Q}}(u) = \frac{1}{4}(a^2 - 5b^2) \in \{-1, +1\}$. Ferner ist $b \neq 0$, denn $b = 0$ hieße $u = \frac{1}{2}a \in \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$, was nicht der Fall ist.

Es ist

$$\{\, u\,,\, u^{-1}\,,\, -u\,,\, -u^{-1} \,\} \;=\; \{\, \frac{1}{2}(a + b\sqrt{5})\,,\, \frac{1}{2}(a - b\sqrt{5})\,,\, \frac{1}{2}(-a - b\sqrt{5})\,,\, \frac{1}{2}(-a + b\sqrt{5}) \,\}\,.$$

Da u das maximale Element dieser Menge ist, folgt $a \geqslant 0$ und $b \geqslant 1$.

Es gibt in $\mathrm{U}(\mathbf{Z}[\alpha]) \cap \mathbf{R}_{>1}$ kein kleineres Element als u, da jedes dieser Elemente eine Potenz von u ist.

Nun ist $a^2 = \pm 4 + 5b^2$, was für jedes dieser Vorzeichen separat monoton in b wächst. Wir suchen also die erste Quadratzahl a^2 in der Folge

$$-4 + 5 \cdot 1^2,\ +4 + 5 \cdot 1^2,\ -4 + 5 \cdot 2^2,\ +4 + 5 \cdot 2^2,\ \ldots$$

Dies führt uns auf $a^2 = -4 + 5 \cdot 1^2 = 1$ und auf $u = \frac{1}{2}(1 + \sqrt{5}) = \alpha$.

Fall $d = 17$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{17})} = \mathbf{Z}[\frac{1}{2}(1 + \sqrt{17})]$; cf. Aufgabe 3. Schreibe $\beta := \frac{1}{2}(1 + \sqrt{17})$.

I.e. es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{17})} = \{\, \frac{1}{2}(a + b\sqrt{17}) \,:\, a, b \in \mathbf{Z},\ a \equiv_2 b \,\}$.

Ist $u = \frac{1}{2}(a + b\sqrt{17}) \in \mathrm{U}(\mathbf{Z}[\beta]) \cap \mathbf{R}_{>1}$ mit $a, b \in \mathbf{Z}$ und $a \equiv_2 b$ gegeben wie in (1), dann ist $\mathrm{N}_{\mathbf{Q}(\beta)|\mathbf{Q}}(u) = \frac{1}{4}(a^2 - 17b^2) \in \{-1, +1\}$. Ferner ist $b \neq 0$, denn $b = 0$ hieße $u = \frac{1}{2}a \in \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$, was nicht der Fall ist.

Es ist

$$\{\, u\,,\, u^{-1}\,,\, -u\,,\, -u^{-1} \,\} \;=\; \{\, \frac{1}{2}(a + b\sqrt{17})\,,\, \frac{1}{2}(a - b\sqrt{17})\,,\, \frac{1}{2}(-a - b\sqrt{17})\,,\, \frac{1}{2}(-a + b\sqrt{17}) \,\}\,.$$

Da u das maximale Element dieser Menge ist, folgt $a \geqslant 0$ und $b \geqslant 1$.

Es gibt in $\mathrm{U}(\mathbf{Z}[\beta]) \cap \mathbf{R}_{>1}$ kein kleineres Element als u, da jedes dieser Elemente eine Potenz von u ist.

Nun ist $a^2 = \pm 4 + 17b^2$, was für jedes dieser Vorzeichen separat monoton in b wächst. Wir suchen also die erste Quadratzahl a^2 in der Folge

$$-4 + 17 \cdot 1^2,\ +4 + 17 \cdot 1^2,\ -4 + 17 \cdot 2^2,\ +4 + 17 \cdot 2^2,\ \ldots$$

Dies führt uns auf $a^2 = -4 + 17 \cdot 2^2 = 64$ und auf $u = \frac{1}{2}(8 + 2\sqrt{17}) = 4 + \sqrt{17}$.

Fall $d = 19$. Es ist $\mathcal{O}_{\mathbf{Q}(\sqrt{19})} = \mathbf{Z}[\sqrt{19}]$; cf. Aufgabe 3.

Ist $u = a + b\sqrt{19} \in \mathrm{U}(\mathbf{Z}[\sqrt{19}]) \cap \mathbf{R}_{>1}$ mit $a, b \in \mathbf{Z}$ gegeben wie in (1), dann ist $\mathrm{N}_{\mathbf{Q}(\sqrt{19})|\mathbf{Q}}(u) = a^2 - 19b^2 \in \{-1, +1\}$. Ferner ist $b \neq 0$, denn $b = 0$ hieße $u = a \in \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$, was nicht der Fall ist.

Es ist

$$\{\, u\,,\, u^{-1}\,,\, -u\,,\, -u^{-1} \,\} \;=\; \{\, a + b\sqrt{19}\,,\, a - b\sqrt{19}\,,\, -a + b\sqrt{19}\,,\, -a - b\sqrt{19}\,,\ \} \,.$$

Da u das maximale Element dieser Menge ist, folgt $a \geqslant 0$ und $b \geqslant 1$.

Es gibt in $\mathrm{U}(\mathbf{Z}[\sqrt{19}]) \cap \mathbf{R}_{>1}$ kein kleineres Element als u, da jedes dieser Elemente eine Potenz von u ist.

Nun ist $a^2 = \pm 1 + 19b^2$, was für jedes dieser Vorzeichen separat monoton in b wächst. Wir suchen also die erste Quadratzahl a^2 in der Folge

$$-1 + 19 \cdot 1^2,\ +1 + 19 \cdot 1^2,\ -1 + 19 \cdot 2^2,\ +1 + 19 \cdot 2^2,\ \ldots$$

Dies führt uns auf $a^2 = 1 + 19 \cdot 39^2 = 28900 = 170^2$ und auf $u = 170 + 39\sqrt{19}$.

Aufgabe 54

Ad (1). Da $v \in \mathrm{U}(\mathcal{O}_K)$ liegt, ist $\mathrm{N}_{K|\mathbf{Q}}(v) \in \mathrm{U}(\mathbf{Z}) = \{-1, +1\}$; cf. Lemma 20.(4). Nach Lemma 15.(2) ist

$$\mathrm{N}_{K|\mathbf{Q}}(v) \ = \ v \cdot \sigma(v) \cdot \bar{\sigma}(v) \ = \ v \cdot |\sigma(v)|^2 \ .$$

Da $v > 1$ und da $|\sigma(v)|^2 > 0$, folgt $\mathrm{N}_{K|\mathbf{Q}}(v) > 0$.

Zusammen erhalten wir $\mathrm{N}_{K|\mathbf{Q}}(v) = 1$.

Somit ist $v \cdot |\sigma(v)|^2 = 1$, i.e. $|\sigma(v)| = v^{-1/2} = x^{-1}$ und also $\sigma(v) = x^{-1}\exp(\mathrm{i}t)$ für ein $t \in [0, 2\pi)$.

Ad (2). Es ist $\mathbf{Z}[v] \subseteq \mathcal{O}_K$. Dank der Aufgaben 14.(3) und 18.(2) wird

$$|\Delta_{K|\mathbf{Q},\,(1,v,v^2)}| \ = \ |\mathbf{Z}[v]^{\#}/\mathbf{Z}[v]| \ = \ |\mathbf{Z}[v]^{\#}/\mathcal{O}_K^{\#}| \cdot |\mathcal{O}_K^{\#}/\mathcal{O}_K| \cdot |\mathcal{O}_K/\mathbf{Z}[v]| \ = \ |\Delta_K| \cdot |\mathcal{O}_K/\mathbf{Z}[v]|^2$$

und also

$$|\Delta_{K|\mathbf{Q},\,(1,v,v^2)}| \ \geqslant \ |\Delta_K| \ .$$

Schreiben wir $c := \cos(t)$, so wird

$$\begin{array}{rcl}
\Delta_K & \overset{\text{B. 25}}{=} & ((v - \sigma(v))(v - \bar{\sigma}(v))(\sigma(v) - \bar{\sigma}(v)))^2 \\
& = & ((x^2 - x^{-1}\mathrm{e}^{\mathrm{i}t})(x^2 - x^{-1}\mathrm{e}^{-\mathrm{i}t})(x^{-1}\mathrm{e}^{\mathrm{i}t} - x^{-1}\mathrm{e}^{-\mathrm{i}t}))^2 \\
& = & ((x^4 - 2x\cos(t) + x^{-2})(2\mathrm{i}x^{-1}\sin(t)))^2 \\
& = & (x^4 - 2xc + x^{-2})^2(-4)x^{-2}(1 - c^2) \\
& = & (-4)(x^3 - 2c + x^{-3})^2(1 - c^2)\ ;.
\end{array}$$

Schreibe $a := x^3 + x^{-3}$. Da $x > 1$ ist, ist $x \neq 0$ und also $x^3 - 2 + x^{-3} = (x^{3/2} - x^{-3/2})^2 > 0$, i.e. $a > 2$. Wir erhalten

$$\frac{1}{4}|\Delta_K| \ = \ (1 - c^2)(a - 2c)^2 \ .$$

Hierbei ist $-1 \leqslant c \leqslant +1$.

Wir suchen den maximalen Wert von

$$f(y) \ := \ (1 - y^2)(a - 2y)^2$$

auf $-1 \leqslant y \leqslant +1$. Da $f(-1) = 0$ und $f(+1) = 0$ sind und da $f(y) > 0$ ist für $-1 < y < +1$, wird der maximale Wert im Inneren dieses Intervalls angenommen. Es ist

$$f'(y) \ = \ -2y \cdot (a - 2y)^2 + (1 - y^2) \cdot 2(-2)(a - 2y) \ = \ 2(4y^2 - ay - 2)(a - 2y) \ ,$$

es ist $f'(y) = 0$ dort genau dann, wenn $y = \frac{1}{8}(a \pm \sqrt{a^2 + 32})$ ist für eines der beiden Vorzeichen. Wegen $a > 2$ ist $a + \sqrt{a^2 + 32} > 8$. Also nimmt f sein Maximum bei $y_0 := \frac{1}{8}(a - \sqrt{a^2 + 32})$ an. Unter Verwendung

von $ay_0 = 4y_0^2 - 2$ wird

$$\begin{aligned}
\tfrac{1}{4}|\Delta_K| &= (1-c^2)(a-2c)^2 \\
&\leqslant f(y_0) \\
&= (1-y_0^2)(a-2y_0)^2 \\
&= (1-y_0^2)(a^2-4ay_0+4y_0^2) \\
&= (1-y_0^2)(a^2+8-12y_0^2) \\
&= a^2+8-20y_0^2+12y_0^4-a^2y_0^2 \\
&= a^2+8-20y_0^2+12y_0^4-16y_0^4+16y_0^2-4 \\
&= a^2+4-4y_0^2-4y_0^4 \\
&= x^6+x^{-6}+6-4y_0^2-4y_0^4 \,.
\end{aligned}$$

Um, wie gewünscht, zu zeigen, daß dies kleiner als $v^3+6 = x^6+6$ ist, genügt es

$$x^{-6} \overset{!}{<} 4y_0^2$$

nachweisen. I.e. wir wollen

$$1 \overset{!}{<} 2|y_0|x^3$$

zeigen.

Aus $x^3 + x^{-3} = a$ folgt $(x^3)^2 - ax^3 + 1 = 0$ und also $x^3 = \frac{1}{2}(a \pm \sqrt{a^2-4})$ für eines der beiden Vorzeichen. *Wäre* dieses Vorzeichen negativ, dann wäre $1 < x^3 = \frac{1}{2}(a - \sqrt{a^2-4})$, i.e. $\sqrt{a^2-4} < a-2$, i.e. $a^2-4 < a^2-4a+4$, i.e. $a < 2$, was *nicht* der Fall ist. Also ist $x^3 = \frac{1}{2}(a+\sqrt{a^2-4})$. Wir erhalten

$$\begin{aligned}
2|y_0|x^3 &= \tfrac{1}{8}(-a+\sqrt{a^2+32})(a+\sqrt{a^2-4}) \\
&= \tfrac{1}{8}(a+\sqrt{a^2+32})^{-1}(-a^2+a^2+32)(a+\sqrt{a^2-4}) \\
&= 4(1+\sqrt{1+32a^{-2}})^{-1}(1+\sqrt{1-4a^{-2}}) \,.
\end{aligned}$$

I.e. es bleibt

$$1+\sqrt{1+32a^{-2}} \overset{!}{<} 4+4\sqrt{1-4a^{-2}}$$

zu zeigen. Es ist $a^{-2} < \frac{1}{4}$. Betrachten wir auf $0 < z \leqslant \frac{1}{4}$ die Funktionen g und h, die durch $g(z) := 1+\sqrt{1+32z}$ und $h(z) := 4+4\sqrt{1-4z}$ gegeben sind, so ist $g(\frac{1}{4}) = 4 = h(\frac{1}{4})$, es ist g streng monoton wachsend und h streng monoton fallend. Damit ist die gewünschte Aussage gezeigt.

Ad (3). Da $K \subseteq \mathbf{R}$ liegt, ist $\{\pm 1\} \leqslant \mu(K) \leqslant \mu(\mathbf{R}) = \{\pm 1\}$, i.e. $\{\pm 1\} = \mu(K)$

Wir wählen einen Gruppenisomorphismus $\{\pm 1\} \times \mathbf{Z}^{\oplus(r+s-1)} = \{\pm 1\} \times \mathbf{Z} \xrightarrow[\sim]{\varphi} \mathrm{U}(\mathcal{O}_K)$, der $(-1,0)$ auf -1 schickt; cf. Satz 126.

In $\{\pm 1\} \times \mathbf{Z}$ sind genau die Elemente $(+1,1)$, $(+1,-1)$, $(-1,1)$, $(-1,-1)$ mit der Eigenschaft ausgestattet, daß sich jedes Element $(\varepsilon, m) \in \{\pm 1\} \times \mathbf{Z}$ eindeutig schreiben läßt als Potenz von diesem Element, multipliziert mit $(+1,0)$ oder mit $(-1,0)$.

Entsprechendes gilt daher in $\mathrm{U}(\mathcal{O}_K)$, wenn wir die vier Elemente $\varphi(\,(+1,1)\,)$, $\varphi(\,(+1,-1)\,)$, $\varphi(\,(-1,1)\,)$, $\varphi(\,(-1,-1)\,)$ betrachten. Sei $\tilde{u} := \varphi(\,(+1,1)\,)$. Dann sind diese vier Elemente gegeben durch $\tilde{u}$, $\tilde{u}^{-1}$, $-\tilde{u}$, $-\tilde{u}^{-1}$. Da $\tilde{u} \notin \{-1,+1\}$ liegt, ist genau eines dieser Elemente größer als 1. Wir nennen es u'.

Somit ist $1 < u'$, und es gibt für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ mit $v \in \{-u'^m, +u'^m\}$.

Sei $u \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < u$ und $4u^{3/2} + 24 \leqslant |\Delta_K|$ gegeben. Wir haben $u \overset{!}{=} u'$ zu zeigen.

Angenommen nicht. Sei $m \in \mathbf{Z}$ mit $u \in \{-u'^m, +u'^m\}$. Da $u > 1$ und $u' > 1$, ist $m \geqslant 1$ und $u = u'^m$. Nach Annahme ist nun $m \geqslant 2$. Also ist

$$|\Delta_K| \overset{(2)}{<} 4u'^3 + 24 \leqslant 4u'^{3m/2} + 24 = 4u^{3/2} + 24 \leqslant |\Delta_K| \,,$$

und wir haben einen *Widerspruch*.

Ad (4). Schreibe $\delta := \sqrt[3]{2}$. Die eingangs gemachten Voraussetzungen an K sind im Falle $K = \mathbf{Q}(\delta)$ erfüllt; cf. Aufgabe 7.

Wie in der Lösung zu (3) gesehen, gibt es genau ein $u \in \mathrm{U}(\mathcal{O}_K)$ so, daß $1 < u$ ist und daß es für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ gibt mit $v \in \{-u^m, +u^m\}$.

Ebenfalls in der Lösung zu (3) gesehen, ist ein $v \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < v$ und $4v^{3/2} + 24 \leqslant |\Delta_K|$, sofern existent, notwendigerweise gleich u.

Wir suchen also ein $v \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < v$ und $4v^{3/2} + 24 \leqslant 108$, i.e. $v \leqslant 21^{2/3}$; cf. Aufgabe 19.(2).

Sei $v := 1 + \delta + \delta^2$. Es ist $1 < v$.

Es ist $(\delta - 1)(1 + \delta + \delta^2) = \delta^3 - 1 = 1$. Also ist $v \in \mathrm{U}(\mathcal{O}_K)$.

Es ist $v \approx 3{,}8473$. Es ist $21^{2/3} \approx 7{,}6117$. Also ist in der Tat $v \leqslant 21^{2/3}$.

Somit folgt $u = v = 1 + \delta + \delta^2 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Ad (5). Es ist $f(X) = X^3 + 2X + 1$. Es ist $f'(X) = 3X^2 + 2$. Es ist $f''(X) = 6X$.

Es ist $f(X)$ irreduzibel, da sein Bild in $\mathbf{F}_3[X]$ mangels Nullstelle in $\mathbf{F}_3$ irreduzibel ist.

Es hat $f(X)$ genau eine reelle Nullstelle, genannt α, da $f''(X)$ die Nullstelle 0 hat und $f'(X) = 3X^2 + 2$ dort positiv ist.

Seien β und $\bar{\beta}$ die weiteren Nullstellen von $f(X)$ in $\mathbf{C}$. Diese liegen nicht in $\mathbf{R}$. Folglich sind die eingangs gemachten Voraussetzungen im Falle $K := \mathbf{Q}(\alpha)$ erfüllt; cf. [**5,** §2.3.4].

Es ist $\alpha^3 = -2\alpha - 1$ und $\alpha^4 = -2\alpha^2 - \alpha$.

Schreibe $\mathrm{Tr} := \mathrm{Tr}_{\mathbf{Q}(\alpha)|\mathbf{Q}}$. Es wird $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\alpha) = \mathrm{tr}\left(\begin{smallmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{smallmatrix}\right) = 0$ und $\mathrm{Tr}(\alpha^2) = \mathrm{tr}\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & 0 & -2 \end{smallmatrix}\right) = -4$. Daraus folgt auch $\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(-2\alpha - 1) = -3$ und $\mathrm{Tr}(\alpha^4) = \mathrm{Tr}(-2\alpha^2 - \alpha) = 8$. Somit wird

$$\Delta_{K|\mathbf{Q},\,(1,\alpha,\alpha^2)} \;=\; \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix} \;=\; \det\begin{pmatrix} 3 & 0 & -4 \\ 0 & -4 & -3 \\ -4 & -3 & 8 \end{pmatrix} \;=\; -59\,.$$

Ergo ist $\Delta_{K|\mathbf{Q},\,(1,\alpha,\alpha^2)}$ quadratfrei, somit also $\mathcal{O}_K = \mathbf{Z}[\alpha]$; cf. Aufgabe 18.(3).

Wie in der Lösung zu (3) gesehen, gibt es genau ein $u \in \mathrm{U}(\mathcal{O}_K)$ so, daß $1 < u$ ist und daß es für alle $v \in \mathrm{U}(\mathcal{O}_K)$ genau ein $m \in \mathbf{Z}$ gibt mit $v \in \{-u^m, +u^m\}$.

Ebenfalls in der Lösung zu (3) gesehen, ist ein $v \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < v$ und $4v^{3/2} + 24 \leqslant |\Delta_K|$, sofern existent, notwendigerweise gleich u.

Wir suchen also ein $v \in \mathrm{U}(\mathcal{O}_K)$ mit $1 < v$ und $4v^{3/2} + 24 \leqslant 59$, i.e. $v \leqslant (35/4)^{2/3}$; cf. Aufgabe 19.(2).

Sei $v := \alpha^2 + 2$. Es ist $1 < v$.

Es ist $\alpha(\alpha^2 + 2) = 1$. Also ist $v \in \mathrm{U}(\mathcal{O}_K)$.

Es ist $f(-\frac{1}{2}) = -\frac{1}{8} < 0$ und $f(0) = 1 > 0$. Also ist $-\frac{1}{2} < \alpha < 0$. Also ist in der Tat

$$v \;=\; 2 + \alpha^2 \;<\; 2{,}25 \;\leqslant\; (35/4)^{2/3} \;\approx\; 4{,}2462\,.$$

Somit folgt $u = v = 2 + \alpha^2$.

Aufgabe 55

Wir machen Gebrauch von $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$; cf. Satz 130.(1). Ferner werden wir Gebrauch machen von der Methode aus der Lösung zu Aufgabe 30.(2), um Primidealfaktorisierungen zu berechnen.

Um in den zu bearbeitenden Fällen zu zeigen, daß $\mathbf{Z}[\zeta_n]$ ein Hauptidealbereich ist, werden wir nachweisen, daß dort $|\mathrm{Cl}(\mathbf{Z}[\zeta_n])| = 1$ gilt; cf. Bemerkung 69.

Ad $n = 3$. In der Notation von Definition 115 ist $k = 2$ und $s = 1$. Ferner ist $|\Delta_{\mathbf{Q}(\zeta_3)}| = 3$; cf. Lemma 129.(4). Somit wird die Minkowskischranke zu

$$\xi_{\mathbf{Q}(\zeta_3)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\zeta_3)}|^{1/2} \;=\; \frac{1}{2} \cdot \frac{4}{\pi} \cdot 3^{1/2} \;\approx\; 1{,}1027\,;$$

cf. Definition 115. Nach Satz 118.(1) müssen für Elemente von $\mathrm{Cl}(\mathbf{Z}[\zeta_3])$ nur Repräsentanten $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\zeta_3])$ mit $|\mathbf{Z}[\zeta_3]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\zeta_3)}$ in Betracht gezogen werden, also nur solche mit $|\mathbf{Z}[\zeta_3]/\mathfrak{a}| = 1$, i.e. nur $\mathfrak{a} = (1)$. Folglich ist $|\mathrm{Cl}(\mathbf{Z}[\zeta_3])| = 1$ und also $\mathbf{Z}[\zeta_3]$ ein Hauptidealbereich.

Ad $n = 4$. In der Notation von Definition 115 ist $k = 2$ und $s = 1$. Ferner ist $|\Delta_{\mathbf{Q}(\zeta_4)}| = 4$; cf. Lemma 129.(4); cf. auch 23. Somit wird die Minkowskischranke zu

$$\xi_{\mathbf{Q}(\zeta_4)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\zeta_4)}|^{1/2} \;=\; \frac{1}{2} \cdot \frac{4}{\pi} \cdot 4^{1/2} \;\approx\; 1{,}2732\,;$$

cf. Definition 115. Nach Satz 118.(1) müssen für Elemente von $\mathrm{Cl}(\mathbf{Z}[\zeta_4])$ nur Repräsentanten $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\zeta_4])$ mit $|\mathbf{Z}[\zeta_4]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\zeta_4)}$ in Betracht gezogen werden, also nur solche mit $|\mathbf{Z}[\zeta_4]/\mathfrak{a}| = 1$, i.e. nur $\mathfrak{a} = (1)$. Folglich ist $|\mathrm{Cl}(\mathbf{Z}[\zeta_4])| = 1$ und also $\mathbf{Z}[\zeta_4] = \mathbf{Z}[\mathrm{i}]$ ein Hauptidealbereich.

Ad $n = 5$. In der Notation von Definition 115 ist $k = 4$ und $s = 2$. Ferner ist $|\Delta_{\mathbf{Q}(\zeta_5)}| = 5^3$; cf. Lemma 129.(4). Somit wird die Minkowskischranke zu

$$\xi_{\mathbf{Q}(\zeta_5)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\zeta_5)}|^{1/2} \;=\; \frac{3}{32} \cdot \left(\frac{4}{\pi}\right)^2 \cdot 5^{3/2} \;\approx\; 1{,}6992\,;$$

cf. Definition 115. Nach Satz 118.(1) müssen für Elemente von $\mathrm{Cl}(\mathbf{Z}[\zeta_5])$ nur Repräsentanten $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\zeta_5])$ mit $\mathbf{Z}[\zeta_5]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\zeta_5)}$ in Betracht gezogen werden, also nur solche mit $|\mathbf{Z}[\zeta_5]/\mathfrak{a}| = 1$, i.e. nur $\mathfrak{a} = (1)$. Folglich ist $|\mathrm{Cl}(\mathbf{Z}[\zeta_5])| = 1$ und also $\mathbf{Z}[\zeta_5]$ ein Hauptidealbereich.

Ad $n = 7$. In der Notation von Definition 115 ist $k = 6$ und $s = 3$. Ferner ist $|\Delta_{\mathbf{Q}(\zeta_7)}| = 7^5$; cf. Lemma 129.(4). Somit wird die Minkowskischranke zu

$$\xi_{\mathbf{Q}(\zeta_7)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\zeta_7)}|^{1/2} \;=\; \frac{5}{324} \cdot \left(\frac{4}{\pi}\right)^3 \cdot 7^{5/2} \;\approx\; 4{,}1295\,;$$

cf. Definition 115. Nach Satz 118.(1) müssen für Elemente von $\mathrm{Cl}(\mathbf{Z}[\zeta_7])$ nur Repräsentanten $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\zeta_7])$ mit $|\mathbf{Z}[\zeta_7]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\zeta_7)}$ in Betracht gezogen werden, also nur solche mit $|\mathbf{Z}[\zeta_7]/\mathfrak{a}| \leqslant 4$.

Bestimmen wir die Primideale $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\zeta_7])$ mit $|\mathbf{Z}[\zeta_7]/\mathfrak{p}| \leqslant 4$. Wegen Primidealfaktorzerlegung und wegen Bemerkung 92 genügt es, diese Primideale als Hauptideale nachzuweisen; cf. Satz 63.(1).

Da $\mathbf{Z}/(\mathfrak{p} \cap \mathbf{Z})$ in $\mathbf{Z}[\zeta_7]/\mathfrak{p}$ einbettet, muß dazu $\mathfrak{p} \cap \mathbf{Z} = (2)$ oder $\mathfrak{p} \cap \mathbf{Z} = (3)$ sein.

Fall $\mathfrak{p} \cap \mathbf{Z} = (2)$. Von $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ zerfällt das Bild $\bar{\Phi}_7(X)$ in $\mathbf{F}_2[X]$ als

$$\bar{\Phi}_7(X) \;=\; (X^3 + X + 1)^1 (X^3 + X^2 + 1)^1$$

in normierte irreduzible Faktoren; cf. auch Satz 131. Folglich ergibt sich in $\mathbf{Z}[\zeta_7]$ die Primidealfaktorzerlegung

$$(2) \;=\; (\zeta_7^3 + \zeta_7 + 1,\, 2)^1 (\zeta_7^3 + \zeta_7^2 + 1,\, 2)^1\,.$$

Da $2/(\zeta_7^3 + \zeta_7 + 1) = -\zeta_7^5 - \zeta_7^3 - \zeta_7^2 - \zeta_7$ ist und da $2/(\zeta_7^3 + \zeta_7^2 + 1) = \zeta_7^5 + \zeta_7^4 + 1$ ist, schreibt sich diese die Primidealfaktorzerlegung als

$$(2) \;=\; (\zeta_7^3 + \zeta_7 + 1)^1 (\zeta_7^3 + \zeta_7^2 + 1)^1\,.$$

Fall $\mathfrak{p} \cap \mathbf{Z} = (3)$. Von $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ zerfällt das Bild $\bar{\Phi}_7(X)$ in $\mathbf{F}_3[X]$ als

$$\bar{\Phi}_7(X) \;=\; (X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^1 \;,$$

ist also irreduzibel; cf. auch Satz 131. Folglich ergibt sich in $\mathbf{Z}[\zeta_7]$ die Primidealfaktorzerlegung

$$(3) \;=\; (3)^1 \;.$$

Somit sind alle fraglichen Primideale als Hauptideale nachgewiesen; cf. Aufgabe 29.(1). Es ist also in der Tat $|\mathrm{Cl}(\mathbf{Z}[\zeta_7])| = 1$ und somit $\mathbf{Z}[\zeta_7]$ ein Hauptidealbereich.

Ad $n = 8$. In der Notation von Definition 115 ist $k = 4$ und $s = 2$. Ferner ist $|\Delta_{\mathbf{Q}(\zeta_8)}| = 2^8$; cf. Lemma 129.(4). Somit wird die Minkowskischranke zu

$$\xi_{\mathbf{Q}(\zeta_8)} \;=\; \frac{k!}{k^k} \cdot \left(\frac{4}{\pi}\right)^s \cdot |\Delta_{\mathbf{Q}(\zeta_8)}|^{1/2} \;=\; \frac{3}{32} \cdot \left(\frac{4}{\pi}\right)^2 \cdot 2^4 \;\approx\; 2{,}4317 \;;$$

cf. Definition 115. Nach Satz 118.(1) müssen für Elemente von $\mathrm{Cl}(\mathbf{Z}[\zeta_8])$ nur Repräsentanten $\mathfrak{a} \in \mathrm{Ideale}^{\times}(\mathbf{Z}[\zeta_8])$ mit $|\mathbf{Z}[\zeta_8]/\mathfrak{a}| \leqslant \xi_{\mathbf{Q}(\zeta_8)}$ in Betracht gezogen werden, also nur solche mit $|\mathbf{Z}[\zeta_8]/\mathfrak{a}| \leqslant 2$.

Bestimmen wir die Primideale $\mathfrak{p} \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(\mathbf{Z}[\zeta_8])$ mit $|\mathbf{Z}[\zeta_8]/\mathfrak{p}| \leqslant 2$. Wegen Primidealfaktorzerlegung und wegen der Bemerkung 92 genügt es, diese Primideale als Hauptideale nachzuweisen; cf. Satz 63.(1).

Da $\mathbf{Z}/(\mathfrak{p} \cap \mathbf{Z})$ in $\mathbf{Z}[\zeta_8]/\mathfrak{p}$ einbettet, muß dazu $\mathfrak{p} \cap \mathbf{Z} = (2)$ sein. Das Bild $\bar{\Phi}_8(X)$ von $\Phi_8(X) = X^4 + 1$ in $\mathbf{F}_2[X]$ zerfällt als

$$\bar{\Phi}_8(X) \;=\; (X + 1)^4$$

in normierte irreduzible Faktoren; cf. auch Satz 131. Folglich ergibt sich in $\mathbf{Z}[\zeta_8]$ die Primidealfaktorzerlegung

$$(2) \;=\; (\zeta_8 + 1,\, 2)^4 \;=\; (1 - \zeta_8\,,\, 2)^4 \;.$$

Da $2/(1 - \zeta_8) = (1 - \zeta_8^4)/(1 - \zeta_8) = \zeta_8^3 + \zeta_8^2 + \zeta_8 + 1$ ist, schreibt sich diese die Primidealfaktorzerlegung als

$$(2) \;=\; (1 - \zeta_8)^4 \;.$$

Somit sind alle fraglichen Primideale als Hauptideale nachgewiesen; cf. Aufgabe 29.(1). Es ist also in der Tat $|\mathrm{Cl}(\mathbf{Z}[\zeta_8])| = 1$ und somit $\mathbf{Z}[\zeta_8]$ ein Hauptidealbereich.

Aufgabe 56

Schreibe $\zeta := \zeta_5$.

Es ist $\mathbf{Z}[\zeta] = \mathcal{O}_{\mathbf{Q}(\zeta)}$; cf. Lemma 129.(2).

Es ist $\mu(\mathbf{Q}(\zeta))$ eine zyklische endliche Gruppe; cf. Lemma 124.(2).

Wir *behaupten*, daß $\mu(\mathbf{Q}(\zeta)) \stackrel{!}{=} \langle\!\langle -\zeta \rangle\!\rangle$ ist. Dazu haben wir $\mu(\mathbf{Q}(\zeta)) \stackrel{!}{\subseteq} \langle\!\langle -\zeta \rangle\!\rangle$ zu zeigen. Es ist $|\langle\!\langle -\zeta \rangle\!\rangle| = 10$. Also ist $\langle\!\langle -\zeta \rangle\!\rangle$ gleich der Menge der Nullstellen von $X^{10} - 1$ in $\mathbf{C}$.

Sei $\eta \in \mu(\mathbf{Q}(\zeta))$. Sei $n := |\langle\!\langle \eta \rangle\!\rangle|$. Wir haben zu zeigen, daß η eine Nullstelle von $X^{10} - 1$ ist, i.e. daß n ein Teiler von 10 ist. Dank der Ordnungen von η und $-\zeta$ gibt es in $\mu(\mathbf{Q}(\zeta))$ ein Element ξ von Ordnung $m := \mathrm{kgV}(n, 10)$; cf. [**5,** Aufgabe 27.(3)]. Wir haben $m \stackrel{!}{=} 10$ zu zeigen.

Es ist $\mathbf{Q}(\xi) \subseteq \mathbf{Q}(\zeta)$ ein Teilkörper. Also ist $[\mathbf{Q}(\xi) : \mathbf{Q}]$ ein Teiler von $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$. Es ist ξ eine Nullstelle von $X^m - 1$. In $\mathbf{C}$ ist also $\xi = \zeta_m^k$ für ein $k \in [0, m-1]$. Da $|\langle\!\langle \xi \rangle\!\rangle| = m$, ist k teilerfremd zu m; cf. [**5,** Aufgabe 27.(2)]. Wähle $a,\, b \in \mathbf{Z}$ mit $ak + bm = 1$. Dann ist $\zeta_m = \zeta_m^{ak+mb} = \xi^a$. Also ist $\mathbf{Q}(\xi) = \mathbf{Q}(\zeta_m)$. Somit ist $\varphi(m) \stackrel{\text{A. 17.(1)}}{=} [\mathbf{Q}(\zeta_m) : \mathbf{Q}]$ ein Teiler von $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$. Schreibe $m := 10 \cdot m' \cdot m'' \cdot m'''$ mit

m', m'', m''' $\in \mathbf{Z}$ derart, daß m' eine Potenz von 2 ist, m'' eine Potenz von 5 und m''' teilerfremd zu 10. Es wird

$$\begin{array}{rcl} \varphi(m) & = & \varphi(10 \cdot m' \cdot m'' \cdot m''') \\ & \overset{\text{B. 128.(3)}}{=} & \varphi(2 \cdot m') \cdot \varphi(5 \cdot m'') \cdot \varphi(m''') \\ & = & \varphi(2 \cdot m') \cdot m'' \cdot 4 \cdot \varphi(m''') \; . \end{array}$$

Da $\varphi(2 \cdot m') > 1$ falls $m' \neq 1$ und da $\varphi(m''') > 1$ falls $m''' \neq 1$, folgt $m' = 1$, $m'' = 1$ und $m''' = 1$, i.e. $m = 10$. Das zeigt die *Behauptung.*

In der Notation von Satz 126 ist $r = 0$ und $s = 2$, und somit $r + s - 1 = 1$. Wir haben diesem Satz zufolge einen Isomorphismus $\varphi : \mu(\mathbf{Q}(\zeta)) \times \mathbf{Z} \xrightarrow{\sim} \mathrm{U}(\mathbf{Z}[\zeta])$, der $(\xi, 0)$ nach ξ abbildet. Sei $\tilde{u} := \varphi((0,1))$. Dann ist jedes Element von $\mathrm{U}(\mathbf{Z}[\zeta])$ von der Form $(-\zeta)^a \tilde{u}^b$ mit eindeutig bestimmten $a \in [0,9]$ und $b \in \mathbf{Z}$.

Diese Eigenschaft bleibt erhalten, wenn wir $\tilde{u}$ ersetzen durch $(-\zeta)^a \tilde{u}$ für ein $a \in \mathbf{Z}$. Sie bleibt auch erhalten, wenn wir $\tilde{u}$ durch $\tilde{u}^{-1}$ ersetzen.

Schreibe $\tilde{\alpha} := \zeta + \zeta^{-1}$. Es ist $\tilde{\alpha}^2 + \tilde{\alpha} - 1 = \zeta^2 + 2 + \zeta^{-2} + \zeta + \zeta^{-1} - 1 = 0$. Also ist $\tilde{\alpha} = \frac{1}{2}(-1 \pm \sqrt{5})$ für eines der beiden Vorzeichen. Da $\mathrm{Re}(\zeta) > 0$, folgt $\tilde{\alpha} = \frac{1}{2}(-1 + \sqrt{5})$. Also ist $\mathbf{Q}(\tilde{\alpha}) \subseteq \mathbf{Q}(\zeta)$.

Schreibe $\alpha := \frac{1}{2}(1 + \sqrt{5}) = \tilde{\alpha} + 1 = \zeta + \zeta^{-1} + 1$. Es ist $\mathbf{Q}(\alpha) = \mathbf{Q}(\tilde{\alpha})$ und $\mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha]$; cf. Aufgabe 3. Es ist $\alpha^2 - \alpha - 1 = 0$, also $\alpha(\alpha - 1) = 1$ und somit $\alpha \in \mathrm{U}(\mathbf{Z}[\alpha]) \leqslant \mathrm{U}(\mathbf{Z}[\zeta])$.

Es ist $\mathbf{Q}(\zeta) \cap \mathbf{R} = \mathbf{Q}(\alpha)$, da $\mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\zeta) \cap \mathbf{R} \subset \mathbf{Q}(\zeta)$ und da es keine Teilkörper von $\mathbf{Q}(\zeta)$ gibt, die echt zwischen $\mathbf{Q}(\alpha)$ und $\mathbf{Q}(\zeta)$ liegen; cf. **[5,** §3.5.2].

Also ist auch $\mathbf{Z}[\zeta] \cap \mathbf{R} = \mathcal{O}_{\mathbf{Q}(\zeta)} \cap \mathbf{R} = \mathcal{O}_{\mathbf{Q}(\zeta)} \cap \mathbf{Q}(\zeta) \cap \mathbf{R} = \mathcal{O}_{\mathbf{Q}(\zeta)} \cap \mathbf{Q}(\alpha) = \mathcal{O}_{\mathbf{Q}(\alpha)} = \mathbf{Z}[\alpha]$. Insbesondere ist auch $\mathrm{U}(\mathbf{Z}[\zeta]) \cap \mathbf{R} = \mathrm{U}(\mathbf{Z}[\alpha])$.

Es besteht $\mathrm{Gal}(\mathbf{Q}(\zeta)|\mathbf{Q}(\alpha))$ aus der Identität und dem Automorphismus $\zeta \mapsto \zeta^{-1}$, da letzterer α festhält; cf. Aufgabe 17.(1). Dieser Automorphismus ist die auf $\mathbf{Q}(\zeta)$ eingeschränkte komplexe Konjugation, da letztere ebenfalls $\zeta \mapsto \zeta^{-1}$ abbildet. Folglich bildet die Normabbildung $\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}(\alpha)}$ ein Element ω aus $\mathbf{Q}(\zeta)$ auf $\omega\bar{\omega} = |\omega|^2$ ab; cf. Korollar 16.(2). Diese schränkt ein auf den Gruppenmorphismus

$$\begin{array}{ccc} \mathrm{U}(\mathbf{Z}[\zeta]) & \longrightarrow & \mathrm{U}(\mathbf{Z}[\alpha]) \\ v & \longmapsto & v\bar{v} \; . \end{array}$$

Es ist jedes Element von $\mathrm{U}(\mathbf{Z}[\alpha])$ von der Form α^c oder $-\alpha^c$ für ein $c \in \mathbf{Z}$; cf. Aufgabe 53.(2). Da $\alpha > 0$ und da $\tilde{u} \cdot \bar{\tilde{u}} = |\tilde{u}|^2 > 0$, folgt

$$\tilde{u}\bar{\tilde{u}} \; = \; \alpha^m$$

für ein $m \in \mathbf{Z}$. Nach eventueller Ersetzung von $\tilde{u}$ durch $\tilde{u}^{-1}$ dürfen wir $m \in \mathbf{Z}_{\geqslant 1}$ annehmen.

Da $\alpha \in \mathrm{U}(\mathbf{Z}[\zeta])$, ist auch umgekehrt

$$\alpha \; = \; (-\zeta)^k \tilde{u}^\ell$$

für ein $k \in [0,9]$ und ein $\ell \in \mathbf{Z}$.

Einsetzen gibt

$$\alpha^{m\ell} = (\tilde{u}\bar{\tilde{u}})^\ell \; = \; (-\zeta)^{-k} \alpha (-\zeta)^k \alpha \; = \; \alpha^2 \; .$$

Also ist $m\ell = 2$. Somit ist $(m, \ell) = (1, 2)$ oder $(m, \ell) = (2, 1)$.

Wir setzen noch $u := (-\zeta)^t \tilde{u}$ mit noch zu spezifizierendem $t \in \mathbf{Z}$. Damit wird

$$\begin{array}{rcl} u\bar{u} & = & \alpha^m \\ \alpha & = & (-\zeta)^{k - t\ell} u^\ell \; . \end{array}$$

Falls $(m, \ell) = (2, 1)$ ist, setzen wir $t = k$. Es folgt $\alpha = u$.

Falls $(m,\ell) = (1,2)$ ist, unterscheiden wir folgende Unterfälle.

Unterfall $k \equiv_2 0$. Wir setzen $t = k/2$. Es folgt $\alpha \stackrel{1.}{=} u \cdot \bar{u} \stackrel{2.}{=} u^2$, also $u = \bar{u}$ reell, also $|u|$ eine ganzzahlige Potenz von α, was wegen $|u| = \alpha^{1/2}$ nicht geht. Dieser Unterfall tritt somit nicht ein.

Unterfall $k \equiv_2 1$. Wir finden $t \in \mathbf{Z}$ mit $t = (5-k)/2$. Es folgt $\alpha \stackrel{1.}{=} u \cdot \bar{u} \stackrel{2.}{=} -u^2$, also $u = -\bar{u}$, i.e. $u \in \mathrm{i}\mathbf{R}$ Unter Verwendung der $\mathbf{Z}$-linearen Basis $(\zeta^{-2}, \zeta^{-1}, \zeta^1, \zeta^2)$ von $\mathbf{Z}[\zeta]$, die sich aus der $\mathbf{Z}$-linearen Basis $(\zeta^0, \zeta^1, \zeta^2, \zeta^3)$ von $\mathbf{Z}[\zeta]$ durch Multiplikation mit ζ und Umsortieren ergibt, schreiben wir $u = z'\zeta^{-2} + y'\zeta^{-1} + y\zeta^1 + z\zeta^2$ mit y, y', z, $z' \in \mathbf{Z}$ und erhalten

$$z'\zeta^{-2} + y'\zeta^{-1} + y\zeta^1 + z\zeta^2 \;=\; u \;=\; -\bar{u} \;=\; -z'\zeta^2 - y'\zeta^1 - y\zeta^{-1} - z\zeta^{-2} \;,$$

i.e.

$$u \;=\; y(\zeta^1 - \zeta^{-1}) + z(\zeta^2 - \zeta^{-2}) \;.$$

Nun gilt

$$\begin{aligned}
-(\zeta + \zeta^{-1}) &= -\alpha \\
&= u^2 \\
&= (y(\zeta^1 - \zeta^{-1}) + z(\zeta^2 - \zeta^{-2}))^2 \\
&= y^2(\zeta^2 - 2 + \zeta^{-2}) + 2yz(\zeta^3 - \zeta^{-1} - \zeta^1 + \zeta^{-3}) + z^2(\zeta^4 - 2 + \zeta^{-4}) \\
&= y^2(2(\zeta + \zeta^{-1}) + 3(\zeta^2 + \zeta^{-2})) + 2yz((\zeta^2 + \zeta^{-2}) - (\zeta^1 + \zeta^{-1})) + z^2(3(\zeta + \zeta^{-1}) + 2(\zeta^2 + \zeta^{-2}))
\end{aligned}$$

und also, durch Koeffizientenvergleich,

$$\begin{aligned}
-1 &= 2y^2 - 2yz + 3z^2 \\
-1 &= 3y^2 + 2yz + 2z^2 \;.
\end{aligned}$$

Aus letzterer Gleichung erhalten wir

$$-\tfrac{1}{2} \;=\; z^2 + yz + \tfrac{3}{2}\,y^2 \;=\; (z + \tfrac{1}{2}\,y)^2 + \tfrac{5}{4}\,y^2 \;,$$

was nicht geht für y, $z \in \mathbf{Z}$. Dieser Unterfall tritt somit auch nicht ein.

Somit ist $\alpha = u$ gezeigt.

Wie das ursprüngliche $\tilde{u}$ hat nun auch $u = \alpha$ die Eigenschaft, daß jedes Element von $\mathrm{U}(\mathbf{Z}[\zeta])$ von der Form $(-\zeta)^a\alpha^b$ ist mit eindeutig bestimmten $a \in [0,9]$ und $b \in \mathbf{Z}$. Insbesondere ist, setzen wir wieder $\alpha = \zeta + \zeta^{-1} + 1$,

$$\mathrm{U}(\mathbf{Z}[\zeta_5]) \;=\; \{\, (-\zeta_5)^a(\zeta_5 + \zeta_5^{-1} + 1)^b \;:\; a \in [0,9],\; b \in \mathbf{Z} \,\}$$

eine Beschreibung von $\mathrm{U}(\mathbf{Z}[\zeta_5])$ wie gesucht.

Aufgabe 57

Schreibe $q := p^{\alpha-1}$. Schreibe $\zeta := \zeta_{pq}$. Schreibe $\underline{z} := (\,\zeta^i \;:\; i \in [0,(p-1)q-1]\,)$.

Wir wiederholen einiges aus dem Beweis zu Lemma 129, manches in etwas präziserer Form.

Es ist

$$\Phi'_{pq}(X) \;=\; (\prod_{k\in U}(X - \zeta^k))' \;=\; \sum_{\ell\in U}\prod_{k\in U\smallsetminus\{\ell\}}(X - \zeta^k) \;,$$

für $m \in U$ also

$$\Phi'_{pq}(\zeta^m) \;=\; \prod_{k\in U\smallsetminus\{m\}}(\zeta^m - \zeta^k) \;.$$

Schreibe $t := (p-1)q((p-1)q-1)/2$. Wir erhalten

$$\begin{array}{rcl}
\Delta_{\mathbf{Q}(\zeta)} & \overset{\text{L. 129.(1, 2)}}{=} & \Delta_{\mathbf{Q}(\zeta)|\mathbf{Q},\,\underline{z}} \\
& \overset{\text{B. 25}}{=} & \prod_{k,\,\ell\,\in\,U,\;k<\ell}(\zeta^\ell-\zeta^k)^2 \\
& = & (-1)^t \prod_{m\in U}\prod_{k\in U\smallsetminus\{m\}}(\zeta^m-\zeta^k) \\
& = & (-1)^t \prod_{m\in U}\Phi'_{pq}(\zeta^m) \\
& \overset{\text{K. 16.(2)}}{=} & (-1)^t\,\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\Phi'_{pq}(\zeta))\;.
\end{array}$$

Aus $\Phi_{pq}(X)(X^q-1) = X^{pq}-1$ folgt durch formales Ableiten

$$\Phi'_{pq}(X)(X^q-1) + \Phi_{pq}(X)\cdot qX^{q-1} \;=\; pqX^{pq-1}$$

und also

$$\Phi'_{pq}(\zeta) \;=\; \frac{pq\zeta^{-1}}{\zeta^q-1}\;;$$

cf. [**5,** Aufgabe 11].

Es ist $\mathrm{Gal}(\mathbf{Q}(\zeta^q)|\mathbf{Q}) \simeq \mathrm{U}(\mathbf{Z}/(p))$ und $\mu_{\zeta^q,\mathbf{Q}}(X) = \Phi_p(X) = \frac{X^p-1}{X-1}$; cf. Aufgabe 17. Also wird

$$\prod_{i\in[1,p-1]}(X-(\zeta^{qi}-1)) \overset{\text{L. 14}}{=} \mu_{\zeta^q-1,\mathbf{Q}}(X) \;=\; \mu_{\zeta^q,\mathbf{Q}}(X+1) \;=\; \Phi_p(X+1) \;=\; \frac{(X+1)^p-1}{(X+1)-1} \;=\; \sum_{i\in[0,p-1]}\tbinom{p}{i+1}X^i\;.$$

Vergleich der konstanten Terme gibt

$$\mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}(\zeta^q-1) \overset{\text{K. 16.(2)}}{=} \prod_{i\in[1,p-1]}(\zeta^{qi}-1) \;=\; (-1)^{p-1}p\;.$$

Gemäß Korollar 16.(2) und Lemma 19.(2) ist

$$\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\zeta^q-1) \;=\; \mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}(\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}(\zeta^q)}(\zeta^q-1)) \;=\; \mathrm{N}_{\mathbf{Q}(\zeta^q)|\mathbf{Q}}((\zeta^q-1)^q) \;=\; (-1)^{(p-1)q}p^q\;.$$

Analog ist der konstante Term von $\Phi_{pq}(X)$ gleich 1 und also

$$\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\zeta) \;=\; (-1)^{(p-1)q}\;.$$

Es folgt

$$\begin{array}{rcl}
\Delta_{\mathbf{Q}(\zeta)} & = & (-1)^t\,\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}(\Phi'_{pq}(\zeta)) \\
& = & (-1)^t\,\mathrm{N}_{\mathbf{Q}(\zeta)|\mathbf{Q}}\left(\frac{pq\zeta^{-1}}{\zeta^q-1}\right) \\
& = & (-1)^t\cdot(pq)^{(p-1)q}\cdot(-1)^{(p-1)q}\cdot(-1)^{(p-1)q}p^{-q} \\
& = & (-1)^t p^{q(\alpha p-\alpha-1)}\;.
\end{array}$$

Fall $p = 2$. Es wird

$$t \;=\; \frac{1}{2}q(q-1) \;\equiv_2\; \partial_{\alpha,1}\;.$$

und also

$$\Delta_{\mathbf{Q}(\zeta_{2^\alpha})} \;=\; (-1)^{\partial_{\alpha,1}}p^{q(\alpha p-\alpha-1)} \;=\; (-1)^{\partial_{\alpha,1}}2^{2^{\alpha-1}(\alpha-1)}\;.$$

Fall $p \geqslant 3$. Es wird

$$\begin{array}{rcl}
t & = & \frac{1}{2}((pq-q)(pq-q-1)) \\
& \equiv_2 & \frac{1}{2}(p^2q^2-pq^2-pq^2+q^2-pq+q) \\
& = & \frac{1}{2}((p^2-p)q^2+(-p+1)(q^2+q)) \\
& \equiv_2 & \frac{1}{2}(p^2-p) \\
& \equiv_2 & \frac{1}{2}(p-1)\;.
\end{array}$$

Wir erhalten

$$\Delta_{\mathbf{Q}(\zeta_{p^\alpha})} \;=\; (-1)^{(p-1)/2} p^{q(\alpha p-\alpha-1)} \;=\; (-1)^{(p-1)/2} p^{p^{\alpha-1}(\alpha p-\alpha-1)} \,.$$

Aufgabe 58

Ad (1). Der Gruppenmorphismus

$$\begin{array}{ccc} \mathbf{F}_p^\times & \xrightarrow{\;\varphi\;} & \mathbf{F}_p^\times \\ x+(p) & \longmapsto & x^2+(p) \end{array}$$

hat den Kern $\langle\!\langle -1+(p)\rangle\!\rangle = \{1+(p), -1+(p)\}$, da das Polynom $X^2-1=0$ in $\mathbf{F}_p$ genau diese beiden Nullstellen hat.

Sein Bild $\varphi(\mathbf{F}_p^\times) = (\mathbf{F}_p^\times)^2$ ist also isomorph zu $\mathbf{F}_p^\times/\langle\!\langle -1+(p)\rangle\!\rangle$. Daher ist $|(\mathbf{F}_p^\times)^2| = (p-1)/2$.

Es ist $\mathbf{F}_p^\times \simeq \mathrm{C}_{p-1}$; cf. [**5,** Aufgabe 27.(5)]. Wähle $g \in \mathbf{Z} \smallsetminus (p)$ mit

$$\mathbf{F}_p^\times = \langle\!\langle g+(p)\rangle\!\rangle \,.$$

Unter dem Gruppenmorphismus

$$\begin{array}{ccc} \mathbf{F}_p^\times & \xrightarrow{\;\psi\;} & \mathbf{F}_p^\times \\ x+(p) & \longmapsto & x^{(p-1)/2}+(p) \end{array}$$

wird $g+(p)$ abgebildet auf ein Element der Ordnung 2; jedes Element wird abgebildet auf ein Element der Ordnung 1 oder 2 ; cf. [**5,** Aufgabe 27.(2)]. Also ist

$$\psi(\mathbf{F}_p^\times) \;=\; \langle\!\langle -1+(p)\rangle\!\rangle \;=\; \mathrm{Kern}(\varphi) \,.$$

Es bildet $\psi \circ \varphi$ alle Elemente auf $1+(p)$ ab; cf. [**5,** Aufgabe 11.(1.c)]. Folglich ist $\varphi(\mathbf{F}_p^\times) \subseteq \mathrm{Kern}(\psi)$. Da $|\varphi(\mathbf{F}_p^\times)| = (p-1)/2$ und auch $|\,\mathrm{Kern}(\psi)| = |\mathbf{F}_p^\times|/|\psi(\mathbf{F}_p^\times)| = (p-1)/2$, folgt

$$(\mathbf{F}_p^\times)^2 \;=\; \varphi(\mathbf{F}_p^\times) \;=\; \mathrm{Kern}(\psi) \,.$$

Sei $a \in \mathbf{Z} \smallsetminus (p)$. Es ist $\psi(a) = 1+(p)$ genau dann, wenn $a \in (\mathbf{F}_p^\times)^2$ liegt, i.e. wenn $\left(\frac{a}{p}\right) = 1$ ist. Es ist $\psi(a) = -1+(p)$ genau dann, wenn $a \notin (\mathbf{F}_p^\times)^2$ liegt, i.e. wenn $\left(\frac{a}{p}\right) = -1$ ist. Jedenfalls ist somit

$$a^{(p-1)/2}+(p) \;=\; \psi(a) \;=\; \left(\tfrac{a}{p}\right)+(p) \,.$$

Seien $a,\, b \in \mathbf{Z} \smallsetminus (p)$. Es wird

$$\begin{array}{rcl} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)+(p) & = & (\left(\frac{a}{p}\right)+(p))(\left(\frac{b}{p}\right)+(p)) \\ & = & (a^{(p-1)/2}+(p))(b^{(p-1)/2}+(p)) \\ & = & (ab)^{(p-1)/2}+(p) \\ & = & \left(\frac{ab}{p}\right)+(p) \,, \end{array}$$

und also auch

$$\left(\tfrac{a}{p}\right)\left(\tfrac{b}{p}\right) \;=\; \left(\tfrac{ab}{p}\right) \,,$$

da $\{-1,+1\} \to \mathbf{Z}/(p)$, $x \mapsto x+(p)$ injektiv ist.

Wähle für jedes $a \in \mathbf{Z} \smallsetminus (p)$ ein $a^* \in \mathbf{Z} \smallsetminus (p)$ mit $a^*+(p) = (a+(p))^{-1}$, i.e. mit $aa^* \equiv_p 1$. Es wird $\left(\frac{a^*}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{aa^*}{p}\right) = \left(\frac{1}{p}\right) = 1$, und somit $\left(\frac{a^*}{p}\right) = \left(\frac{a}{p}\right)$.

Ad (2). Schreibe $\bar{a} := a+(p)$ für $a \in \mathbf{Z}$. Schreibe $U := \mathrm{U}(\mathbf{Z}/(p))$ und $U^{\neq 1} := \mathrm{U}(\mathbf{Z}/(p)) \smallsetminus \{\bar{1}\}$.

Sei wieder $\mathbf{F}_p^\times = \langle\!\langle g + (p) \rangle\!\rangle$ für ein geeignetes $g \in \mathbf{Z} \smallsetminus (p)$. Es ist

$$\begin{array}{rcl} -\sum_{c+(p)\in U} \left(\frac{c}{p}\right) & = & \left(\frac{g}{p}\right) \sum_{c+(p)\in U} \left(\frac{c}{p}\right) \\ & \overset{(1)}{=} & \sum_{c+(p)\in U} \left(\frac{gc}{p}\right) \\ & \overset{d=gc}{=} & \sum_{d+(p)\in U} \left(\frac{d}{p}\right) \\ & = & \sum_{c+(p)\in U} \left(\frac{c}{p}\right), \end{array}$$

und also $\sum_{c+(p)\in U} \left(\frac{c}{p}\right) = 0$, i.e. $\sum_{c+(p)\in U^{\neq 1}} \left(\frac{c}{p}\right) = -\left(\frac{1}{p}\right) = -1$.

Damit wird

$$\begin{array}{rcl} \tau^2 & = & (\sum_{\bar a\in U} \left(\frac{a}{p}\right)\zeta_p^a)(\sum_{\bar b\in U} \left(\frac{b}{p}\right)\zeta_p^b) \\ & = & \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{a}{p}\right)\zeta_p^a\left(\frac{b}{p}\right)\zeta_p^b \\ & \overset{(1)}{=} & \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{ab}{p}\right)\zeta_p^{a+b} \\ & = & \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{-ab}{p}\right)\zeta_p^{a-b} \\ & = & \left(\frac{-1}{p}\right) \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{ab}{p}\right)\zeta_p^{a-b} \\ & = & \left(\frac{-1}{p}\right) \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{ab}{p}\right)\zeta_p^{a-b} \\ & \overset{(1)}{=} & \left(\frac{-1}{p}\right) \sum_{\bar a,\,\bar b\,\in\, U} \left(\frac{ab^*}{p}\right)\zeta_p^{a-b} \\ & \overset{\bar c = \bar a\bar b^{-1}}{=} & \left(\frac{-1}{p}\right) \sum_{\bar c,\,\bar b\,\in\, U} \left(\frac{c}{p}\right)\zeta_p^{bc-b} \\ & \overset{\bar d = \bar b(\bar c - 1)}{=} & \left(\frac{-1}{p}\right)\left(\left(\sum_{\bar c\in U^{\neq 1}} \left(\frac{c}{p}\right) \sum_{\bar b\in U} \zeta_p^{b(c-1)}\right) + \left(\sum_{\bar b\in U} \left(\frac{1}{p}\right)\zeta^0\right)\right) \\ & = & \left(\frac{-1}{p}\right)\left(\left(\sum_{\bar c\in U^{\neq 1}} \left(\frac{c}{p}\right) \sum_{\bar d\in U} \zeta_p^{d}\right) + (p-1)\right) \\ & = & \left(\frac{-1}{p}\right)\left(-\left(\sum_{\bar c\in U^{\neq 1}} \left(\frac{c}{p}\right)\right) + (p-1)\right) \\ & = & \left(\frac{-1}{p}\right)(1 + (p-1)) \\ & = & \left(\frac{-1}{p}\right)p\,. \end{array}$$

Ad (3). Dank (2) gibt es in $\mathbf{Q}(\zeta_p)$ eine Nullstelle des Polynoms $X^2 - \left(\frac{-1}{p}\right)p$.

Also liegen beide komplexe Nullstellen dieses Polynoms in $\mathbf{Q}(\zeta_p)$, namentlich $+\sqrt{\left(\frac{-1}{p}\right)p}$ und $-\sqrt{\left(\frac{-1}{p}\right)p}$, welche Wurzel man in $\mathbf{C}$ dazu auch immer gewählt hat.

Somit ist $\mathbf{Q}(\sqrt{\left(\frac{-1}{p}\right)p})$ ein Teilkörper von $\mathbf{Q}(\zeta_p)$.

Aufgabe 59

Ad (1). Es ist $\left(\frac{-1}{23}\right) = (-1)^{(23-1)/2} = -1$; cf. Aufgabe 58.(1).

Gemäß Aufgabe 58.(3) ist $\mathbf{Q}(\sqrt{\left(\frac{-1}{23}\right)23}) = \mathbf{Q}(\sqrt{-23})$ ein Teilkörper von $\mathbf{Q}(\zeta_{23})$.

Ad (2). Es ist $\mathcal{O}_{\mathbf{Q}(\zeta_{23})} \overset{\text{L. 129.(2)}}{=} \mathbf{Z}[\zeta_{23}]$. Es ist ferner

$$\mathcal{O}_{\mathbf{Q}(\zeta_{23})} \;=\; \Gamma_{\mathbf{Q}(\zeta_{23})}(\mathbf{Z}) \;\overset{\text{A. 5.(2)}}{=}\; \Gamma_{\mathbf{Q}(\zeta_{23})}(\Gamma_{\mathbf{Q}(\sqrt{-23})}(\mathbf{Z})) \;=\; \Gamma_{\mathbf{Q}(\zeta_{23})}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})})\,.$$

Gemäß Aufgabe 47.(1) ist $\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})}) \simeq \mathrm{C}_3$.

Insbesondere ist $3 = |\mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})})|$ teilerfremd zu $[\mathbf{Q}(\zeta_{23}) : \mathbf{Q}(\sqrt{-23})] = 11$.

Wir können also Aufgabe 50.(3) zum Einsatz bringen und erhalten den surjektiven Gruppenmorphismus

$$\begin{array}{ccc} \mathrm{Cl}(\mathbf{Z}[\zeta_{23}]) & \xrightarrow{\mathrm{N}_{\mathbf{Q}(\zeta_{23})|\mathbf{Q}(\sqrt{-23})}} & \mathrm{Cl}(\mathcal{O}_{\mathbf{Q}(\sqrt{-23})}) \\ [\mathfrak{h}] & \longmapsto & [\mathrm{N}_{\mathbf{Q}(\zeta_{23})|\mathbf{Q}(\sqrt{-23})}(\mathfrak{h})] \; . \end{array}$$

Sei $[\mathfrak{g}]$ ein Urbild eines Elements der Ordnung 3 unter diesem Gruppenmorphismus. Dann ist 3 ein Teiler der Ordnung von $[\mathfrak{g}]$. Folglich ist 3 ein Teiler der Ordnung von $\mathrm{Cl}(\mathbf{Z}[\zeta_{23}])$.

Insbesondere ist $|\mathrm{Cl}(\mathbf{Z}[\zeta_{23}])| > 1$ und folglich $\mathbf{Z}[\zeta_{23}]$ kein Hauptidealbereich; cf. Bemerkung 69.(1).

Aufgabe 60

Ad (1). Zunächst ist $\Delta_{\mathbf{Q}(\zeta_{40})} = \Delta^4_{\mathbf{Q}(\zeta_8)} \cdot \Delta^4_{\mathbf{Q}(\zeta_5)}$; cf. Satz 130.(2).

Das Vorzeichen von $\Delta_{\mathbf{Q}(\zeta_8)}$ und von $\Delta_{\mathbf{Q}(\zeta_5)}$ spielt also keine Rolle, es genügt also, mittels Lemma 129.(4) festzustellen, daß $|\Delta_{\mathbf{Q}(\zeta_8)}| = 2^8$ und $|\Delta_{\mathbf{Q}(\zeta_5)}| = 5^3$ ist.

So erhalten wir $\Delta_{\mathbf{Q}(\zeta_{40})} = 2^{32} \cdot 5^{12}$.

Ad (2). Wir schreiben $\zeta := \zeta_{40}$.

Es ist $\Phi_{40}(X) = X^{16} - X^{12} + X^8 - X^4 + 1$.

Das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_2[X]$ zerfällt gemäß Satz 131 in $d = 1$ normierten irreduziblen Faktor von Grad $f = 4$ mit Exponent $e = 4$. In der Tat wird

$$X^{16} - X^{12} + X^8 - X^4 + 1 \; = \; (X^4 + X^3 + X^2 + X + 1)^4 \; \in \; \mathbf{F}_2[X]$$

die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_2[X]$. Das liefert die Primidealfaktorzerlegung

$$(2) \; = \; (\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1,\, 2)^4 \; .$$

Das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_3[X]$ zerfällt gemäß Satz 131 in $d = 4$ normierte irreduziblen Faktoren von Grad $f = 4$ mit Exponent $e = 1$. In der Tat wird

$$X^{16}-X^{12}+X^8-X^4+1 \; = \; (X^4+X^2+X+1)(X^4+X^2-X+1)(X^4+X^3+X^2+1)(X^4-X^3+X^2+1) \; \in \; \mathbf{F}_3[X]$$

die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_3[X]$. Das liefert die Primidealfaktorzerlegung

$$(3) \; = \; (\zeta^4 + \zeta^2 + \zeta + 1,\, 3)(\zeta^4 + \zeta^2 - \zeta + 1,\, 3)(\zeta^4 + \zeta^3 + \zeta^2 + 1,\, 3)(\zeta^4 - \zeta^3 + \zeta^2 + 1,\, 3) \; .$$

Das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_5[X]$ zerfällt gemäß Satz 131 in $d = 2$ normierte irreduziblen Faktoren von Grad $f = 2$ mit Exponent $e = 4$. In der Tat wird

$$X^{16} - X^{12} + X^8 - X^4 + 1 \; = \; (X^2 + 2)^4 (X^2 - 2)^4 \; \in \; \mathbf{F}_5[X]$$

die Zerlegung in normierte irreduzible Faktoren in $\mathbf{F}_5[X]$. Das liefert die Primidealfaktorzerlegung

$$(5) \; = \; (\zeta^2 + 2,\, 5)^4 (\zeta^2 - 2,\, 5)^4 \; .$$

Ad (3).

1. Damit das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_p[X]$ irreduzibel ist, sollte, in der Notation von Satz 131, $d = 1$ und $e = 1$ sein.

Für $e = 1$ brauchen wir $p \notin \{2, 5\}$.

Für $d = 1$ brauchen wir dann $f = 16$. Die Restklasse von p in $\mathbf{Z}/(40)$ sollte also in $\mathrm{U}(\mathbf{Z}/(40))$ von Ordnung 16 sein.

Nun ist aber $\mathrm{U}(\mathbf{Z}/(40)) \simeq \mathrm{U}(\mathbf{Z}/(8)) \times \mathrm{U}(\mathbf{Z}/(5))$; cf. Bemerkung 128.(3). Nun ist aber $\mathrm{U}(\mathbf{Z}/(8)) \simeq \mathrm{C}_2 \times \mathrm{C}_2$ und $\mathrm{U}(\mathbf{Z}/(5)) \simeq \mathrm{C}_4$. Jedes Element in $\mathrm{U}(\mathbf{Z}/(40))$ hat also eine Ordnung, die 4 teilt.

Somit gibt es keine Primzahl p, für welche das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_p[X]$ irreduzibel ist.

2. Damit das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_p[X]$ in Linearfaktoren zerfällt, sollte, in der Notation von Satz 131, $f = 1$ sein.

Die Restklasse von p in $\mathbf{Z}/(40)$ sollte also in $\mathrm{U}(\mathbf{Z}/(40))$ von Ordnung 1 sein. Dies ist genau dann der Fall, wenn $p \equiv_{40} 1$ ist.

Somit zerfällt das Bild von $\Phi_{40}(X)$ in $\mathbf{F}_p[X]$ genau dann in Linearfaktoren, wenn $p \equiv_{40} 1$ ist.

Dies ist e.g. für $p \in \{41, 241, 281, 401, 521, 601, 641, 761, 881\}$ der Fall.

Aufgabe 61

Schreibe $\mathcal{O}_L = \mathbf{Z}[y]$ für ein geeignetes $y \in \mathcal{O}_L$, was nach Voraussetzung möglich ist.

Sei $p \in \mathbf{Z}_{>0}$ prim.

Wir verwenden die Bezeichnungen von §4.2.2 im Falle $A = \mathbf{Z}$, $K = \mathbf{Q}$ und $\mathfrak{p} = (p)$.

Es ist $G_\mathfrak{q}/I_\mathfrak{q} \simeq \mathrm{Gal}(\bar{B}|\bar{A})$; cf. Satz 143.(2). Da $\bar{A} \simeq \mathbf{F}_p$ ist und $\bar{B}|\bar{A}$ eine endliche Körpererweiterung nach Aufgabe 43.(1), ist $\mathrm{Gal}(\bar{B}|\bar{A})$ zyklisch; cf. **[5,** §3.6].

Damit (p) bezüglich $K|\mathbf{Q}$ Zerlegungsbreite $d = 1$ hat, sollte $L_{\mathrm{dec}} = K$, i.e. $G_\mathfrak{q} = G$ sein; cf. Satz 143.(1), Definition 137.(1), **[5,** §3.5.2].

Da G nichtzyklisch ist, sollte wegen $G_\mathfrak{q}/I_\mathfrak{q}$ zyklisch dazu $I_\mathfrak{q} \neq 1$ sein, i.e. $e > 1$; cf. Satz 143.(3).

Letzteres kann aber nur der Fall sein, wenn p ein Teiler von $\Delta_{L|K,\,(b^0,\ldots,b^{\ell-1})}$ ist.

Nun hat aber $\Delta_{L|K,\,(b^0,\ldots,b^{\ell-1})}$ nur endlich viele Primteiler.

Aufgabe 62

Wir schreiben auch $L := \mathbf{Q}(\delta, \zeta)$, $M := \mathbf{Q}(\delta)$ und $K := \mathbf{Q}$. Also $L|M|K$.

Ad (1). Es ist $\mu_{\delta,K}(X) = X^3 - 2$; cf. Lösung zu Aufgabe 7.(1). Also ist $\mu_{\delta+1,K}(X) = (X-1)^3 - 2 = X^3 - 3X^2 + 3X - 3$.

Insbesondere ist $(\delta+1)((\delta+1)^2 - 3(\delta+1) + 3(\delta+1)) = 3$, i.e. $(\delta+1)^{-1} = \frac{1}{3}((\delta+1)^2 - 3(\delta+1) + 3) = \frac{1}{3}(\delta^2 - \delta + 1)$.

Es ist $\mu_{\zeta,K}(X) = \Phi_3(X) = X^2 + X + 1$. Also ist $\mu_{\zeta-1,K}(X) = (X+1)^2 + (X+1) + 1 = X^2 + 3X + 3$.

Es sind $\mathbf{Q}(\zeta)|\mathbf{Q}$ und $\mathbf{Q}(\delta)|\mathbf{Q}$ linear disjunkt. Denn es ist $\mathbf{Q}(\delta, \zeta)$ ein Kompositum von $\mathbf{Q}(\zeta)|\mathbf{Q}$ und $\mathbf{Q}(\delta)|\mathbf{Q}$ vermöge der Einbettungen, und es ist $[\mathbf{Q}(\zeta, \delta) : \mathbf{Q}] = 6 = 2 \cdot 3 = [\mathbf{Q}(\zeta) : \mathbf{Q}] \cdot [\mathbf{Q}(\delta) : \mathbf{Q}]$; cf. Lemma 44.

Also ist auch $\mu_{\zeta-1,M}(X) = \mu_{\zeta-1,\mathbf{Q}(\delta)}(X) = X^2 + 3X + 3$; cf. Definition 43.

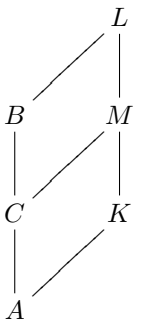
Sei

$$\eta \;:=\; \frac{\zeta - 1}{\delta + 1}\,.$$

Es ist

$$\begin{aligned}
\mu_{\eta,M}(X) &= \mu_{\eta,\mathbf{Q}(\delta)}(X) \\
&= (((\delta+1)X)^2 + 3((\delta+1)X) + 3)(\delta+1)^{-2} \\
&= X^2 + (\delta^2 - \delta + 1)X + \tfrac{1}{3}(\delta^2 - \delta + 1)^2 \;=\; X^2 + (\delta^2 - \delta + 1)X + (\delta^2 - 1)\,.
\end{aligned}$$

Schreibe $A := \mathbf{Z}$, $C := \mathcal{O}_M$ und $B := \mathcal{O}_L$; cf. Aufgabe 19.(2). Es ist $C = \mathbf{Z}[\delta]$, und dies ist ein Hauptidealbereich; cf. Aufgaben 19.(2) und 48.



Somit ist $\eta \in \Gamma_L(C) = \Gamma_L(\Gamma_M(A)) \overset{\text{A. 5.(2)}}{=} \Gamma_L(\mathbf{Z}) = \mathcal{O}_L = B$.

Es ist $\frac{\zeta^2-1}{\delta+1} = (\zeta+1)\,\frac{\zeta-1}{\delta+1} = (\zeta+1)\eta$.

Also wird

$$\Delta_{L|M,\,(1,\eta)} \overset{\text{B. 25}}{=} ((\zeta+1)\eta-\eta)^2 \;=\; (\zeta\eta)^2 \;=\; \zeta^2\,\frac{(\zeta-1)^2}{(\delta+1)^2} \;=\; \zeta^2(\zeta^2-2\zeta+1)\frac{1}{3}(\delta^2-1) \;=\; 1-\delta^2\,.$$

Es ist

$$\mathrm{N}_{M|K}(1-\delta^2) \overset{\text{L. 15.(2)}}{=} (1-\delta^2)(1-(\zeta\delta)^2)(1-(\zeta^2\delta)^2) \;=\; 1-\delta^6 \;=\; -3\,.$$

Also ist $1-\delta^2 \in C$ irreduzibel. Da C ein Hauptidealbereich ist, folgt $1-\delta^2$ prim; cf. Aufgabe 2.(2).

Es wird

$$C[\eta] \;\subseteq\; B \;\subseteq\; B^{\#,C} \;\subseteq\; C[\eta]^{\#,C}\,;$$

cf. Bemerkung 30, Lemma 31, §2.3.4.

Es ist $\underline{y} = (\,y_1\,,\,y_2\,) := (1,\eta)$ eine C-lineare Basis von $C[\eta]$. Sei $\underline{g} = (\,g_1\,,\,g_2\,)$ eine C-lineare Basis von B; cf. Lemma 33.

Sei $\underline{y'} = (\,y'_1\,,\,y'_2\,)$ die zu $\underline{y}$ und $\underline{g'} = (\,g'_1\,,\,g'_2\,)$ die zu $\underline{g}$ duale Basis bezüglich der Spurbilinearform von $L|M$; cf. Lemma 22.

Schreibe $y_i = \sum_{j\in[1,2]} g_j\,s_{j,i}$ für $i \in [1,2]$, wobei $S := (s_{i,\,j})_{i,\,j} \in C^{2\times 2}$. I.e. S ist die beschreibende Matrix der C-linearen Einbettungsabbildung $C[\eta] \hookrightarrow B$ bezüglich $\underline{y}$ und $\underline{g}$.

Wir *behaupten,* daß für $i \in [1,2]$

$$g'_i \overset{!}{=} \sum_{j\in[1,n]} s_{i,\,j}\,y'_j\,.$$

ist. Für $k \in [1,2]$ wird auf der einen Seite

$$\mathrm{Tr}_{L|M}(g'_i\cdot y_k) \;=\; \textstyle\sum_{j\in[1,2]}\,\mathrm{Tr}_{L|M}(g'_i\cdot g_j)s_{j,k} \;=\; \sum_{j\in[1,2]}\partial_{i,\,j}\,s_{j,k} \;=\; s_{i,k}\,,$$

auf der anderen Seite

$$\mathrm{Tr}_{L|M}(\textstyle\sum_{j\in[1,2]}s_{i,\,j}\,y'_j\cdot y_k) \;=\; \sum_{j\in[1,2]}s_{i,\,j}\;\mathrm{Tr}_{L|M}(y'_j\cdot y_k) \;=\; \sum_{j\in[1,2]}s_{i,\,j}\,\partial_{j,k} \;=\; s_{i,k}\,,$$

also beidesmal dasselbe. Dies zeigt die *Behauptung,* da die Spurbilinearform nichtausgeartet ist; cf. Lemma 22. I.e. S^{t} ist die beschreibende Matrix der C-linearen Einbettungsabbildung $B^{\#,C} \hookrightarrow C[\eta]^{\#,C}$ bezüglich $\underline{g'}$ und $\underline{y'}$.

Schreibe $g_i = \sum_{j\in[1,2]} g'_j\, d_{j,i}$ für $i \in [1,2]$, wobei $D := (d_{i,j})_{i,j} \in C^{2\times 2}$. I.e. D ist die beschreibende Matrix der C-linearen Einbettungsabbildung $B \hookrightarrow B^{\#,C}$ bezüglich $\underline{g}$ und $\underline{g'}$.

Wir *behaupten,* daß für $i \in [1,2]$ sich $d_{i,j} = \mathrm{Tr}_{L|M}(g_i \cdot g_j)$ ergibt, mithin also $\Delta_{L|M,\,\underline{g}} = \det(D)$. Für $i,\, k \in [1,2]$ wird

$$\begin{aligned}\mathrm{Tr}_{L|M}((\textstyle\sum_{j\in[1,2]} g'_j\ \mathrm{Tr}_{L|M}(g_i\cdot g_j))g_k) &= \textstyle\sum_{j\in[1,2]} \mathrm{Tr}_{L|M}(g_i\cdot g_j)\,\mathrm{Tr}_{L|M}(g'_j\cdot g_k)\\ &= \textstyle\sum_{j\in[1,2]} \mathrm{Tr}_{L|M}(g_i\cdot g_j)\partial_{j,k}\\ &= \mathrm{Tr}_{L|M}(g_i\cdot g_k)\ .\end{aligned}$$

Da die Spurbilinearform nichtausgeartet ist, folgt $\sum_{j\in[1,2]} g'_j\ \mathrm{Tr}_{L|M}(g_i\cdot g_j) = g_i$ für $i \in [1,2]$; cf. Lemma 22. Dies zeigt die *Behauptung.*

Da die Einbettung $C[\eta] \hookrightarrow C[\eta]^{\#,C}$ die beschreibende Matrix $S^{\mathrm{t}}DS$ besitzt bezüglich $\underline{y}$ und $\underline{y'}$, wird genauso $\Delta_{L|M,\,\underline{y}} = \det(S^{\mathrm{t}}DS) = \det(S)^2\det(D)$.

Da aber $\Delta_{L|M,\,\underline{y}} = 1-\delta^2$ prim ist, folgt, daß $\det(S) \in \mathrm{U}(C)$ liegt; cf. Aufgabe 2. Also ist die Einbettungsabbildung $C[\eta] \hookrightarrow B$ bijektiv, i.e. $C[\eta] = B$. Mit anderen Worten, es ist

$$\mathcal{O}_{\mathbf{Q}(\delta,\zeta)} \;=\; \mathcal{O}_L \;=\; B \;=\; C[\eta] \;=\; \mathbf{Z}[\delta,\eta]\ .$$

Insbesondere ist $\underline{h} := (\eta^0\delta^0, \eta^0\delta^1, \eta^0\delta^2, \eta^1\delta^0, \eta^1\delta^1, \eta^1\delta^2)$ eine $\mathbf{Z}$-lineare Basis von $\mathcal{O}_{\mathbf{Q}(\delta,\zeta)}$.

Cf. Aufgaben 18 und 14.

Beachte auch $\mathbf{Z}[\delta,\zeta] \subset B$, da $\eta \in B$, aber $\eta = (\delta+1)^{-1}\zeta - (\delta+1)^{-1} \notin \mathbf{Z}[\delta,\zeta]$, da $\delta+1 \notin \mathrm{U}(C)$, da $\mathrm{N}_{M|K}(\delta+1) = 3 \notin \mathrm{U}(A)$, wie wir $\mu_{\delta+1,K}(X)$ entnehmen; cf. Lemma 14.

Nach Satz 100.(2) und Lemma 96 wird, als Ideale in $\mathbf{Z}$,

$$\begin{aligned}(\Delta_{L|K,\,\underline{h}}) &\overset{\text{L. 96}}{=} \mathfrak{d}_{L|K,A}\\ &\overset{\text{S. 100.(2)}}{=} \mathrm{N}_{M|K}(\mathfrak{d}_{L|M,C})\cdot\mathfrak{d}^2_{M|K,A}\\ &\overset{\text{L. 96}}{=} \mathrm{N}_{M|K}(\,(\Delta_{L|M,(1,\eta)})\,)\cdot(\Delta_{M|K,(1,\delta,\delta^2)})^2\\ &\overset{\text{A. 19.(2), B. 86.(3)}}{=} (\,\mathrm{N}_{M|K}(\Delta_{L|M,(1,\eta)})\,)\cdot(-2^2\cdot 3^3)^2\\ &\overset{\text{s.o.}}{=} (-3)\cdot(-2^2\cdot 3^3)^2\\ &= (2^4\cdot 3^7)\ .\end{aligned}$$

In anderen Worten, es ist

$$|\Delta_{\mathbf{Q}(\delta,\zeta)}| \;=\; |\Delta_L| \;=\; 2^4\cdot 3^7\ .$$

Beachte, daß wir wegen $\Delta_{\mathbf{Q}(\zeta)} = -3$ und $\Delta_{\mathbf{Q}(\delta)} = -108$ nicht teilerfremd den Satz 48 nicht zur Anwendung bringen können. Und in der Tat ist sowohl

$$\mathbf{Z}[\delta,\zeta] \subset \mathcal{O}_{\mathbf{Q}(\delta,\zeta)}$$

als auch

$$|\Delta_{\mathbf{Q}(\delta,\eta)}| \;=\; 3^7\cdot 2^4 \;\neq\; 3^9\cdot 2^4 \;=\; (3^3\cdot 2^2)^2\cdot 3^3 \;=\; |\Delta_{\mathbf{Q}(\delta)}|^{[\mathbf{Q}(\zeta):\mathbf{Q}]}\cdot|\Delta_{\mathbf{Q}(\zeta)}|^{[\mathbf{Q}(\delta):\mathbf{Q}]}\ ,$$

so daß die Aussagen des Satzes hier in der Tat nicht zutreffen.

Ad (2). Wir gehen in zwei Schritten vor, zerlegen zunächst (5) in $\mathbf{Z}[\delta] = \mathcal{O}_M$ und dann das Resultat weiter in $\mathbf{Z}[\delta,\eta] = \mathcal{O}_L$, unter Verwendung der Lösung zu Aufgabe 30.(2).

In $\mathbf{F}_5[X]$ ist

$$X^3 - 2 \;=\; (X+2)^1(X^2-2X-1)^1$$

die Zerlegung in normierte irreduzible Faktoren. In $\mathbf{Z}[\delta]$ erhalten wir also die Primidealfaktorzerlegung

$$(5) \;=\; (\delta+2,5)(\delta^2-2\delta-1,5)\;.$$

Wir haben Körperisomorphismen

$$\begin{array}{ccccc} \mathbf{Z}[\delta]/(\delta+2,5) & \xrightarrow{\sim} & \mathbf{F}_5[X]/(\bar{\mu}_{\delta,K}(X), X+2) & \xrightarrow{\sim} & \mathbf{F}_5 \\ \delta & \longmapsto & X & \longmapsto & -2\;. \end{array}$$

In $(\mathbf{Z}[\delta]/(\delta+2,5))[X]$ haben wir das Bild von $\mu_{\eta,M}(X) = X^2 + (\delta^2-\delta+1)X + (\delta^2-1)$ unter der koeffizientenweisen Restklassenabbildung in normierte irreduzible Faktoren zu zerlegen. Unter dem koeffizientenweise angewandten ebengenannten Isomorphismus wird dieses Bild zu

$$X^2 + ((-2)^2 - (-2) + 1)X + ((-2)^2 - 1) \;=\; X^2 + 2X - 2\;.$$

In $\mathbf{F}_5[X]$ haben wir die Faktorisierung

$$X^2 + 2X - 2 \;=\; (X^2+2X-2)^1$$

in normierte irreduzible Faktoren. Also erhalten in $\mathbf{Z}[\delta,\eta]$ die Primidealfaktorzerlegung

$$(\delta+2,5) \;=\; (\delta+2,5)^1\;.$$

Schreibe $\mathfrak{q} := (\delta+2,5)$. Damit ist der Verzweigungsindex von (5) bezüglich $L|K$ gleich 1, denn die Zerlegung des anderen Faktors $(\delta^2-2\delta-1,5)$ in $\mathbf{Z}[\delta,\eta]$ kann nicht das Primideal $(\delta+2,5)$ enthalten, wie der Schnitt mit $\mathbf{Z}[\delta]$ zeigt.

Wir erinnern an $\mathrm{Gal}(L|K) = \{\,\tau_i \,:\, i \in [1,6]\,\} = \mathrm{S}_3$ (nach Identifikation) aus der Lösung zur Aufgabe 7.(1). Es beläßt τ_4 die Erzeuger von $(\delta+2,5) \subseteq \mathbf{Z}[\delta,\eta]$ und bildet damit dieses Ideal auf sich ab. Also ist $\tau_4 \in G_{\mathfrak{q}}$. Es kann aber nicht $G_{\mathfrak{q}} = \mathrm{S}_3$ sein, da diesenfalls dank Lemma 138.(1) das Ideal (5) in $\mathbf{Z}[\delta,\eta]$ Zerlegungsbreite 1 haben müßte, was schon in $\mathbf{Z}[\delta]$ nicht der Fall war. Also muß $G_{\mathfrak{q}} = \langle\!\langle \tau_4 \rangle\!\rangle$ sein.

Da $\mathrm{S}_3 = G_{\mathfrak{q}} \sqcup \tau_2 G_{\mathfrak{q}} \sqcup \tau_3 G_{\mathfrak{q}}$ ist, haben wir dank Lemma 138.(1) in $\mathbf{Z}[\delta,\eta]$ die Primidealfaktorzerlegung

$$(5) \;=\; \mathfrak{q}^1 \cdot \tau_2(\mathfrak{q})^1 \cdot \tau_3(\mathfrak{q})^1 \;=\; (\delta+2,5)^1(\zeta\delta+2,5)^1(\zeta^2\delta+2,5)^1\;.$$

Somit ergibt sich die Zerlegungsbreite von (5) zu

$$d \;=\; 3\;.$$

Da der Verzweigungsindex

$$e \;=\; 1$$

ist und da $d\,e\,f = [L:K] = 6$ sein muß, folgt

$$f \;=\; 2\,;$$

cf. Lemma 138.(4).

In der Tat ergibt auch eine direkte Rechnung in $\mathbf{Z}[\delta,\eta]$

$$\begin{aligned} (\zeta\delta+2,5)(\zeta^2\delta+2,5) &= (\,\delta^2-2\delta+4\,,\,5\zeta\delta+10\,,\,5\zeta^2\delta+10\,,\,25\,) \\ &= (\,\delta^2-2\delta+4\,,\,(\delta^2-2\delta+4)(\delta+2)\,,\,5\zeta\delta+10\,,\,5\zeta^2\delta+10\,,\,25\,) \\ &= (\,\delta^2-2\delta+4\,,\,10\,,\,5\zeta\delta+10\,,\,5\zeta^2\delta+10\,,\,25\,) \\ &= (\,\delta^2-2\delta+4\,,\,10\,,\,5\zeta\delta+10\,,\,5\zeta^2\delta+10\,,\,5\,) \\ &= (\,\delta^2-2\delta-1\,,\,5\,)\,, \end{aligned}$$

und wir haben so in der Tat den anderen Primidealfaktor der obengenannten Zerlegung von (5) in $\mathbf{Z}[\delta]$ dann im Ring $\mathbf{Z}[\delta,\eta]$ weiter in zwei Primidealfaktoren zerlegt.

Aus (1) wissen wir bereits, daß (5) teilerfremd zu $|\Delta_M| = 108$ ist, der Verzweigungsindex aller Primidealfaktoren von (5) bezüglich $M|K$ also gleich 1 ist; cf. Lemma 136.

Ferner ist $(\Delta_{L|M,\,(1,\eta)}) = (1-\delta^2)$ teilerfremd zu $(\delta+2,5)$ und zu $(\delta^2-2\delta-1,5)$, da ansonsten die Idealnormen bezüglich $M|K$ einen gemeinsamen Primidealfaktor in $\mathbf{Z}$ hätten, diese sind aber auf der einen Seite gleich (3), auf der anderen Seite jeweils eine Potenz von (5) ; cf. Aufgabe 34.(3) oder Aufgabe 43.(1) (genauer, (5^1) resp. (5^2)). Also haben beide Faktoren $(\delta+2,5)$ und $(\delta^2-2\delta-1,5)$ bezüglich $L|M$ den Verzweigungsindex 1 ; cf. Lemma 136.

Insgesamt hat (5) bezüglich $L|K$ den Verzweigungsindex 1 – wie unsere direkte Rechnung ja auch bestätigt hat.

Ad (3). Sei, wie in (2), das Primideal $\mathfrak{q} = (\delta+2,5) \subseteq \mathbf{Z}[\delta,\eta]$ betrachtet. Es ist, wie dort ermittelt, $G_\mathfrak{q} = \langle\!\langle \tau_4 \rangle\!\rangle$. Also ist der Zerlegungskörper von $\mathfrak{q}$ bezüglich $L|K$ gegeben durch

$$L_{\mathrm{dec}} \;=\; \mathrm{Fix}_{G_\mathfrak{q}}(L) \;=\; M \;=\; \mathbf{Q}(\delta)\,;$$

cf. Aufgabe 7.(1).

Ferner ist $[L : L_{\mathrm{inert}}] = e = 1$; cf. Satz 143.(3). Also ist

$$L_{\mathrm{inert}} \;=\; L \;=\; \mathbf{Q}(\delta,\zeta)\,.$$

Ad (4). Die Aussagen sind falsch. Wir haben mit $(1,2,3)$ unter Beibehaltung der dortigen Notation nun folgendes Gegenbeispiel.

Es ist $K = \mathbf{Q}$, $A = \mathbf{Z}$, $L = \mathbf{Q}(\delta,\zeta) = \mathbf{Q}(\delta,\eta)$, $B = \mathbf{Z}[\delta,\eta]$, $L_{\mathrm{dec}} = \mathbf{Q}(\delta)$ und $B_{\mathrm{dec}} = \mathbf{Z}[\delta]$.

Sei $\mathfrak{p} = (5) \in \mathrm{Ideale}^{\times}_{\mathrm{prim}}(A)$. Wir haben $\mathfrak{q} = (\delta+2,5)$ gewählt.

Sei $\mathfrak{r} = (\delta^2-2\delta-1,5)$. Es ist der Trägheitsindex von $\mathfrak{r}$ bezüglich $L_{\mathrm{dec}}|K$ gleich 2.

Die Zerlegungsbreite von (5) bezüglich $L|K$ ist gleich $d = 3$. Die Zerlegungsbreite von (5) bezüglich $L_{\mathrm{dec}}|K$ ist dagegen gleich 2.

Aufgabe 63

Ad (1).

Schreibe $G := \mathrm{Gal}(\mathbf{Q}(\zeta)|\mathbf{Q})$. Schreibe $K := \mathbf{Q}$ und $L := \mathbf{Q}(\zeta)$.

Unabhängigkeiten von der Wahl. Seien $\mathfrak{q}$ und $\tilde{\mathfrak{q}}$ Primideale von B, die 3 enthalten, die also in der Primidealfaktorzerlegung von (3) auftreten; cf. Aufgabe 29.(1).

Gemäß Lemma 138.(1) gibt es ein $\sigma \in G$ mit $\sigma(\mathfrak{q}) = \tilde{\mathfrak{q}}$. Dann gilt für die Zerlegungsgruppen

$$\begin{aligned}
G_{\tilde{\mathfrak{q}}} &= G_{\sigma(\mathfrak{q})} \\
&= \{\,\rho \in G \,:\, \rho\sigma(\mathfrak{q}) = \sigma(\mathfrak{q})\,\} \\
&= \{\,\rho \in G \,:\, \sigma^{-1}\rho\sigma(\mathfrak{q}) = \mathfrak{q}\,\} \\
&= \{\,\rho \in G \,:\, \sigma^{-1}\rho\sigma \in G_\mathfrak{q}\,\} \\
&= \{\,\rho \in G \,:\, \rho \in \sigma \circ G_\mathfrak{q} \circ \sigma^{-1}\,\} \\
&= \sigma G_\mathfrak{q} \sigma^{-1}\,.
\end{aligned}$$

Da aber G abelsch ist, folgt $G_{\tilde{\mathfrak{q}}} = \sigma \circ G_\mathfrak{q} \circ \sigma^{-1} = G_\mathfrak{q}$.

Für die Zerlegungskörper gilt entsprechend $L_{\mathrm{dec},\mathfrak{q}} = \mathrm{Fix}_{G_\mathfrak{q}}(L) = \mathrm{Fix}_{G_{\tilde{\mathfrak{q}}}}(L) = L_{\mathrm{dec},\tilde{\mathfrak{q}}}$; cf. Definition 137.(1).

Nun gilt ferner für die Trägheitsgruppen

$$\begin{array}{rcl} I_{\tilde{\mathfrak{q}}} & = & I_{\sigma(\mathfrak{q})} \\ & = & \{\, \rho \in G_{\sigma(\mathfrak{q})} \,:\, \rho(b) \equiv_{\sigma(\mathfrak{q})} b \text{ für } b \in B \,\} \\ & = & \{\, \rho \in G_{\sigma(\mathfrak{q})} \,:\, \rho(b) - b \in \sigma(\mathfrak{q}) \text{ für } b \in B \,\} \\ & = & \{\, \rho \in G_{\sigma(\mathfrak{q})} \,:\, \sigma^{-1}(\rho(b) - b) \in \mathfrak{q} \text{ für } b \in B \,\} \\ & = & \{\, \rho \in \sigma \circ G_{\mathfrak{q}} \circ \sigma^{-1} \,:\, \sigma^{-1}(\rho(b)) \equiv_{\mathfrak{q}} \sigma^{-1}(b) \text{ für } b \in B \,\} \\ & = & \{\, \tau \in G_{\mathfrak{q}} \,:\, \sigma^{-1}((\sigma \circ \tau \circ \sigma^{-1})(b)) \equiv_{\mathfrak{q}} \sigma^{-1}(b) \text{ für } b \in B \,\} \\ & = & \{\, \tau \in G_{\mathfrak{q}} \,:\, \tau(\sigma^{-1}(b)) \equiv_{\mathfrak{q}} \sigma^{-1}(b) \text{ für } b \in B \,\} \\ & \overset{\text{L. 20.(1)}}{=} & \{\, \tau \in G_{\mathfrak{q}} \,:\, \tau(\tilde{b}) \equiv_{\mathfrak{q}} \tilde{b} \text{ für } \tilde{b} \in B \,\} \\ & = & I_{\mathfrak{q}} \,, \end{array}$$

selbst ohne G abelsch verwendet zu haben.

Für die Trägheitskörper gilt entsprechend $L_{\text{inert},\mathfrak{q}} = \text{Fix}_{I_{\mathfrak{q}}}(L) = \text{Fix}_{I_{\tilde{\mathfrak{q}}}}(L) = L_{\text{inert},\tilde{\mathfrak{q}}}$; cf. Definition 137.(1).

Berechnung von Zerlegungs- und Trägheitskörper. Es ist $\Phi_{24}(X) = X^8 - X^4 + 1 \in \mathbf{Z}[X]$. Die Zerlegungsparameter sind, in den Bezeichnungen von Satz 131, Verzweigungsindex $e = 2$, Trägheitsgrad $f = 2$ und Zerlegungsbreite $d = 2$. Damit im Einklang hat sein Bild $\bar{\Phi}_{24}(X)$ in $\mathbf{F}_3[X]$ folgende Zerlegung in normierte irreduzible Faktoren.

$$\bar{\Phi}_{24}(X) \;=\; X^8 - X^4 + 1 \;=\; X^8 + 2X^4 + 1 \;=\; (X^4 + 1)^2 \;=\; (X^2 + X - 1)^2 (X^2 - X - 1)^2 \;\in\; \mathbf{F}_3[X]$$

Folglich erhalten wir die Primidealfaktorzerlegung in B

$$(3) \;=\; (\zeta^2 + \zeta - 1,\, 3)^2 (\zeta^2 - \zeta - 1,\, 3)^2$$

cf. Lösung zu Aufgabe 30.(2). Wähle $\mathfrak{q} := (\zeta^2 + \zeta - 1,\, 3)$.

Wir haben den Isomorphismus

$$\begin{array}{rcl} B/\mathfrak{q} & \overset{\psi}{\xrightarrow{\sim}} & \mathbf{F}_3[X]/(X^2 + X - 1) \\ \zeta + \mathfrak{q} & \longmapsto & X + (X^2 + X - 1) \end{array}$$

cf. Lösung zu Aufgabe 30.(2).

Schreibe $U := \{1, 5, 7, 11, 13, 17, 19, 23\}$. Schreiben wir $\sigma_i : L \xrightarrow{\sim} L$, $\zeta \mapsto \zeta^i$ für $i \in U$. Dann ist

$$G \;=\; \{\, \sigma_i \,:\, i \in U \,\} \,;$$

cf. Aufgabe 17.(1). Die Zerlegungsgruppe wird

$$\begin{array}{rcl} G_{\mathfrak{q}} & = & \{\, \sigma \in G \,:\, \sigma(\mathfrak{q}) = \mathfrak{q} \,\} \\ & \overset{\sigma(\mathfrak{q}) \text{ max.}}{=} & \{\, \sigma \in G \,:\, \sigma(\mathfrak{q}) \subseteq \mathfrak{q} \,\} \\ & = & \{\, \sigma \in G \,:\, \sigma(\zeta^2 + \zeta - 1) \in \mathfrak{q} \,\} \\ & = & \{\, \sigma_i \in G \,:\, i \in U,\, \zeta^{2i} + \zeta^i - 1 \in \mathfrak{q} \,\} \\ & \overset{\psi \text{ Isom.}}{=} & \{\, \sigma_i \in G \,:\, i \in U,\, X^{2i} + X^i - 1 \in (X^2 + X - 1) \text{ in } \mathbf{F}_3[X] \,\} \\ & = & \{\, \sigma_1 \,,\, \sigma_{11} \,,\, \sigma_{17} \,,\, \sigma_{19} \,\} \,. \end{array}$$

A priori ist $[L_{\text{dec}} : K] = d = 2$; cf. Satz 143.(1). Ferner ist $L_{\text{dec}} = \text{Fix}_{G_{\mathfrak{q}}}(L) \ni \sigma_1(\zeta) + \sigma_{11}(\zeta) + \sigma_{17}(\zeta) + \sigma_{19}(\zeta) = -\zeta^5 - \zeta^3 + \zeta$ von Minimalpolynom $\mu_{-\zeta^5 - \zeta^3 + \zeta}(X) = X^2 + 2$. Folglich ist bereits $L_{\text{dec}} = \mathbf{Q}(\sqrt{-2})$, wobei wir $\sqrt{-2}$ mit $-\zeta^5 - \zeta^3 + \zeta$ identifizieren wollen.

In den Bezeichnungen von Definition 137 ist also $B_{\text{dec}} = \mathbf{Z}[\sqrt{-2}]$; cf. Aufgabe 3.

Schreibe $U_{\mathrm{dec}} = \{1, 11, 17, 19\}$. Die Trägheitsgruppe wird

$$\begin{array}{rcl} I_{\mathfrak{q}} & = & \{\, \sigma \in G_{\mathfrak{q}} \,:\, \sigma(b) \equiv_{\mathfrak{q}} b \text{ für } b \in B \,\} \\ & = & \{\, \sigma \in G_{\mathfrak{q}} \,:\, \sigma(\zeta) \equiv_{\mathfrak{q}} \zeta \,\} \\ & = & \{\, \sigma_i \in G \,:\, i \in U_{\mathrm{dec}}\,,\, \zeta^i \equiv_{\mathfrak{q}} \zeta \,\} \\ & = & \{\, \sigma_i \in G \,:\, i \in U_{\mathrm{dec}}\,,\, \zeta^i - \zeta \in \mathfrak{q} \,\} \\ \overset{\psi \text{ Isom.}}{} & = & \{\, \sigma_i \in G \,:\, i \in U_{\mathrm{dec}}\,,\, X^i - X \in (X^2 + X - 1) \text{ in } \mathbf{F}_3[X] \,\} \\ & = & \{\, \sigma_1\,,\, \sigma_{17} \,\}\,. \end{array}$$

A priori ist $[L : L_{\mathrm{inert}}] = e = 2$; cf. Satz 143.(3). Ferner ist $L_{\mathrm{inert}} = \mathrm{Fix}_{I_{\mathfrak{q}}}(L) \ni \zeta^3$, da $3 \cdot 17 = 51 \equiv_{24} 3$. Es ist $[\mathbf{Q}(\zeta^3) : \mathbf{Q}] = [\mathbf{Q}(\zeta_8) : \mathbf{Q}] = 4$; cf. Aufgabe 17.(1). Folglich ist $[L : \mathbf{Q}(\zeta^3)] = 2$. Also ist bereits $L_{\mathrm{inert}} = \mathbf{Q}(\zeta_8)$.

In den Bezeichnungen von Definition 137 ist also $B_{\mathrm{inert}} = \mathbf{Z}[\zeta^3]$; cf. Lemma 129.(2).

Ad (2). In $\mathbf{F}_3[X]$ haben wir die folgende Zerlegung in normierte irreduzible Faktoren.

$$X^2 + 2 \;=\; (X-1)(X+1) \;\in\; \mathbf{F}_3[X]\,.$$

Folglich haben wir in $B_{\mathrm{dec}} = \mathbf{Z}[\sqrt{-2}]$ die Primidealfaktorisierung

$$(3) \;=\; (\sqrt{-2} - 1,\, 3)(\sqrt{-2} + 1,\, 3)\,.$$

cf. Lösung zu Aufgabe 30.(2). Dabei ist $\sqrt{-2}-1 = -\zeta^5-\zeta^3+\zeta-1 \in \mathfrak{q}$, da $-X^5-X^3+X-1 \in (X^2+X-1)$ in $\mathbf{F}_3[X]$. Folglich ist

$$\mathfrak{q}_{\mathrm{dec}} \;=\; (\sqrt{-2} - 1,\, 3) \;=\; (\sqrt{-2} - 1)\,,$$

wobei letzteres wegen $(\sqrt{-2} - 1)(-\sqrt{-2} - 1) = 3$ gilt.

In der Tat ist $\mathrm{v}_{\mathfrak{q}_{\mathrm{dec}}}(\,(3)\,) = 1$, wie in Satz 143.(1) behauptet.

Ferner ist $\bar{B}_{\mathrm{dec}} = B_{\mathrm{dec}}/(\sqrt{-2}-1,\, 3) \xrightarrow{\sim} \mathbf{F}_3[X]/(X-1) \xrightarrow{\sim} \mathbf{F}_3$, wobei $\sqrt{-2}$ auf X und dann auf 1 abgebildet wird; cf. Lösung zu Aufgabe 30.(2).

Ad (3). Es ist $\mu_{\zeta^3,\mathbf{Q}}(X) = X^4+1$. In $\mathbf{Q}(\sqrt{-2})[X]$ haben wir dann $X^4+1 = (X^2-X\sqrt{-2}-1)(X^2+X\sqrt{-2}-1)$. Es ist $(\zeta^3)^2 + \zeta^3\sqrt{-2} - 1 = \zeta^6 + \zeta^3(-\zeta^5 - \zeta^3 + \zeta) - 1 = 0$, und also $\mu_{\zeta^3,\mathbf{Q}(\sqrt{-2})}(X) = X^2 + X\sqrt{-2} - 1$. Sein Bild $\bar{\mu}_{\zeta^3,\mathbf{Q}(\sqrt{-2})}(X)$ in $\mathbf{F}_3[X]$ zerfällt wie folgt in ein Produkt normierter irreduzibler Faktoren.

$$\bar{\mu}_{\zeta^3,\mathbf{Q}(\sqrt{-2})}(X) \;=\; (X^2 + X - 1)^1 \;\in\; \mathbf{F}_3[X]\,.$$

Folglich haben wir $B_{\mathrm{inert}} = \mathbf{Z}[\zeta^3]$ die Primidealfaktorisierung

$$B_{\mathrm{inert}}\mathfrak{q}_{\mathrm{dec}} = (\sqrt{-2} - 1) \;=\; \mathfrak{q}_{\mathrm{inert}}\,;$$

cf. Lösung zu Aufgabe 30.(2).

In der Tat wird dies von Satz 143.(2) so ausgesagt.

Ferner ist $\bar{B}_{\mathrm{inert}} = B_{\mathrm{inert}}/(\sqrt{-2}-1) \xrightarrow{\sim} \mathbf{F}_3[T]/(T^2+T-1)$, $\zeta^3 + (\sqrt{-2}-1) \mapsto T + (T^2+T-1)$; cf. Lösung zu Aufgabe 30.(2). Schreibe darin $t := T + (T^2 + T - 1)$. Es wird also $\zeta^3 + (\sqrt{-2} - 1) \mapsto t$ abgebildet. Ferner ist $\mathbf{F}_3[T]/(T^2 + T - 1) = \mathbf{F}_3(t) \simeq \mathbf{F}_9$. Darin gilt $t^2 = 1 - t$.

Ad (4). Es ist $\zeta^8 - \zeta^4 + 1 = 0$ und also $\zeta^{10} - \zeta^6 + \zeta^2 = 0$. Folglich ist $\mu_{\zeta,\mathbf{Q}(\zeta^3)}(X) = X^2 + \zeta^9 X - \zeta^6$. Sein Bild $\bar{\mu}_{\zeta,\mathbf{Q}(\zeta^3)}(X)$ in $\mathbf{F}_3(t)[X]$ zerfällt wie folgt in ein Produkt normierter irreduzibler Faktoren.

$$\bar{\mu}_{\zeta,\mathbf{Q}(\zeta^3)}(X) \;=\; X^2 + t^3 X - t^2 \;=\; X^2 + 2(t+1)X + (t-1) \;=\; (X + (t+1))^2$$

Folglich haben wir $B = \mathbf{Z}[\zeta]$ die Primidealfaktorisierung

$$B\mathfrak{q}_{\mathrm{inert}} = (\sqrt{-2} - 1) \;=\; (\zeta + \zeta^3 + 1,\, 3)^2\,;$$

cf. Lösung zu Aufgabe 30.(2).

Somit muß $(\zeta^2+\zeta-1,\,3)=\mathfrak{q}=(\zeta+\zeta^3+1,\,3)$ sein. Zur Probe verifizieren wir zum einen

$$\zeta+\zeta^3+1 \;=\; (\zeta-1)(\zeta^2+\zeta-1)+3\zeta \;\in\; (\zeta^2+\zeta-1,\,3)\;,$$

zum andern

$$\zeta^2+\zeta-1 \;=\; (-\zeta^7-\zeta^6-\zeta^5-\zeta^4)(\zeta+\zeta^3+1)+3(\zeta^7+\zeta^6+\zeta^5+\zeta^4-1) \;\in\; (\zeta+\zeta^3+1,\,3)\;.$$

Ferner ist nun $B\mathfrak{q}_{\text{inert}}=\mathfrak{q}^2=\mathfrak{q}^e$ erkannt, wie von Satz 143.(3) ausgesagt.

Aufgabe 64

Schreibe $\bar a := a+(p)$ für $a\in\mathbf{Z}$. Sei, wie in Aufgabe 58, $\tau := \sum_{\bar a\in \mathrm{U}(\mathbf{Z}/(p))}\left(\frac{a}{p}\right)\zeta_p^a$.

Nach Aufgabe 58.(1) ist für $b\in\mathbf{Z}\smallsetminus(\ell)$

$$b^{(\ell-1)/2} \;\equiv_\ell\; \left(\tfrac{b}{p}\right)\;.$$

Zum einen wird also

$$\begin{array}{rcl}\tau^\ell & = & \tau(\tau^2)^{\frac{\ell-1}{2}}\\ & \overset{\text{A. 58.(2)}}{=} & \tau\left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}}p^{\frac{\ell-1}{2}}\\ & \equiv_\ell & \tau(-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right)\;.\end{array}$$

Zum anderen wird, unter Verwendung dessen, daß Potenzieren mit ℓ den Frobenius-Ringmorphismus auf dem Ring $\mathbf{Z}[\zeta_p]/(\ell)$ liefert, cf. [**5,** A. 24.(1)],

$$\begin{array}{rcl}\tau^\ell & \equiv_\ell & \sum_{\bar a\in \mathrm{U}(\mathbf{Z}/(p))}\left(\frac{a}{p}\right)^\ell\zeta_p^{a\ell}\\ & = & \sum_{\bar a\in \mathrm{U}(\mathbf{Z}/(p))}\left(\frac{a}{p}\right)\zeta_p^{a\ell}\\ & = & \left(\frac{\ell}{p}\right)\sum_{\bar a\in \mathrm{U}(\mathbf{Z}/(p))}\left(\frac{a\ell}{p}\right)\zeta_p^{a\ell}\\ & \overset{\bar{\tilde a}=\bar a\bar\ell}{=} & \left(\frac{\ell}{p}\right)\sum_{\tilde a\in \mathrm{U}(\mathbf{Z}/(p))}\left(\frac{\tilde a}{p}\right)\zeta_p^{\tilde a}\\ & = & \left(\frac{\ell}{p}\right)\tau\;.\end{array}$$

Multiplikation mit τ liefert

$$\tau^2(-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\tfrac{p}{\ell}\right) \;\equiv_\ell\; \tau^2\left(\tfrac{\ell}{p}\right)\;.$$

Da $\tau^2 \overset{\text{A. 58.(2)}}{=} \left(\frac{-1}{p}\right)p \not\equiv_\ell 0$, repräsentiert τ^2 ein invertierbares Element von $\mathbf{Z}/(\ell)$ und damit auch ein invertierbares Element von $\mathbf{Z}[\zeta_p]/(\ell)$. Somit wird

$$(-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\tfrac{p}{\ell}\right) \;\equiv_\ell\; \left(\tfrac{\ell}{p}\right)\;.$$

Wegen $\ell\geqslant 3$ folgt

$$(-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\tfrac{p}{\ell}\right) \;=\; \left(\tfrac{\ell}{p}\right)\;,$$

und also

$$\left(\tfrac{p}{\ell}\right)\left(\tfrac{\ell}{p}\right) \;=\; (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\;.$$

Literatur

[1] Atiyah, M.F., Macdonald, I.G., Commutative Algebra, Addison-Wesley, 1969.

[2] Conrad, K., *Dirichlet's unit theorem,* www.math.uconn.edu/~kconrad/blurbs/gradnumthy/unittheorem.pdf, 2006 (Zugriff 29.01.2015).

[3] dito, *The splitting field of* X^3-2 *over* $\mathbf{Q}$*,* www.math.uconn.edu/~kconrad/blurbs/gradnumthy/Qw2.pdf, 2006 (Zugriff 02.04.2015).

[4] Künzer, M., *Computeralgebra,* Skript, Stuttgart, 2011.

[5] dito, *Galoistheorie,* Skript, Koblenz, 2009.

[6] dito, *Gewöhnliche Darstellung endlicher Gruppen,* Skript, Stuttgart, 2013.

[7] dito, *Homologische Algebra,* Skript, Bremen, 2010.

[8] dito, *Kommutative Algebra,* Skript, Stuttgart, 2018.

[9] dito, *Topologie,* Skript, Koblenz, 2009.

[10] Masley, J.M., Montgomery, H.L., *Cyclotomic fields with unique factorisation,* J. reine angew. Math. 286-287, S. 248-256.

[11] Neukirch, J., *Algebraische Zahlentheorie,* Springer, 1992.

Folgende Webfundstellen fanden Verwendung. Zugriffe im Wintersemester 2014/15.

```
en.wikipedia.org/wiki/Cyclotomic_field
math.stackexchange.com/questions/261828/class-group-of-mathbbq-sqrt-47
math.stackexchange.com/questions/873941/
 finding-ideal-representatives-in-the-class-group-of-mathbbq-zeta-23
```

Alle angeführten Skripte finden sich auf
`w5.mathematik.uni-stuttgart.de/fachbereich/Kuenzer/Kuenzer/manuscripts.html` .